EJLT European Journal of Law and Technology

Stalking the Stranger in Web 2.0: A Contemporary Regulatory Analysis

Subhajit Basu [1]

Cite as: Basu, S, 'Stalking the Stranger in Web 2.0: A Contemporary Regulatory Analysis', European Journal for Law and Technology, Vol. 3, No. 2, 2012

Abstract

Cyberstalking is an important issue which causes significant distress but which has been difficult to find a means of regulating, particularly through formal criminal systems. Yet proper regulation of cyberstalking behaviour could have substantial impact upon the wellbeing of many victims – from child to adult. In this article, I suggest that a different from of regulation is required: one based upon a virtual, community-based concept of regulation. Such a concept offers a novel approach based on three elements fundamental to the discussion of regulation of cyberstalking: (1) the differences between physical stalking and cyberstalking; (2) the character of a virtual community and the effects of social interactions; and (3) the scope of experience and reality. This formulation is based on an expansive view of regulation and 'normativity' of a virtual community. The author advocates the formation of codes of conduct based on the 'rights and responsibilities' discourse, termed here as 'protocols,' which reflect optimal sociological conceptions. The philosophical underpinning of protocols recognises the value of community, essentially the connection between individuals and their community. As such, these protocols will assist in the formation of private laws that are practical and acceptable within the virtual community. The aim of this concept of regulation is to ensure that cyberspace remains a lawful and socially useful space.

1. Introduction

This article explores the differences between physical stalking and cyberstalking and critically analyses how these differences affect the nature of regulation. In this article, the term cyberstalking refers to conduct occurring by users of the internet, which is threatening or unwanted statements or advances directed at another user of the technology. In contrast, stalking, as discussed in this article, refers to 'a series of acts which are intended to, or in fact, cause harassment to another person'. [2] As a result of these distinctions, I argue in favour of a more expansive view of regulation [3] of cyberstalking in Web2.0 specifically within virtual communities. [4] [5] In doing so, I define and develop the status of 'protocols' – declarations of best practices as a form and source of private law, articulated and negotiated in response to practical detail within a virtual community. [6] The philosophical basis of 'protocols' is similar to 'communitarianism,' particularly 'responsive communitarianism,' which essentially values the connection between an individual and community. [7] [8] Providing the choice of control to a virtual community will ensure that the current hierarchal concept of regulation moves toward more optimal sociological conceptions – 'protocols.' [9]

This proposal is designed in the spirit of pragmatism to ensure that cyberspace remains a lawful and socially useful space. This may appear to be a *prima facie* critique of the existing system of regulation. It is not. I am concerned not with designing formal legal reforms, but with a more fundamental problem: the approach to regulation of cyberstalking. What is needed is regulation based on a deeper understanding of the culture of 'virtuality' and thus, a deeper awareness of the nature and manifestations of cyberstalking behaviour. As I will demonstrate, there are good reasons, both pragmatic and jurisprudential, for favouring this approach. I am also not suggesting that reform of existing laws is unimportant. However, in the context of cybercrime, analysts such as Fafinski, Dutton and Margetts have recognised that the emancipatory potential of international and national law has, to say the least, proven disappointing. [10] Critics argue that cyberspace in its present form is full of laws with little supporting evidence to prove their efficacy in compelling users to

act lawfully. [11] Reform has been compromised and limited. In general, criminal activities in cyberspace have not only replicated those in the physical world but have also taken on their own character, fuelled by an environment where anonymity is the norm.[12] [13] Further, the new social technologies have altered the underlying architecture of social interaction and information distribution.

The remarkable proliferation of Web 2.0 social software platforms such as Facebook, Bebo, MySpace, and Second Life [14] has resulted in commoditization of social relations [15] *and* personal information. [16] [17]Consequently, people are encouraged to post their personal profiles, interests, blogs, photos, videos and online diaries, often sharing thoughts and desires they would otherwise keep secret. [18] Such personal information provides insight into the fantasies, insecurities, and alter egos of people. [19] Arguably, this large-scale divulgence of personal information [20] facilitates and thereby encourages cyberstalking. [21] The ability to cyber-stalk has also increased because of geolocative social networking tools such as 'Foursquare' [22] and the use of intelligent systems that enable much more sophisticated data-mining. [23] [24] Such environments actively encourage users to share personal information, and sophisticated tools enable the capture and analysis of a vast expanse of information. [25] But opportunity and ease alone do not fully account for deviant behaviour. [26] The problem at present is that existing policies intended to prevent cybercrimes are ineffective and leave victims unprotected. [27]

A typical legal article proposing regulation of cyberstalking rarely looks into cyberspace with any real social insight; instead, such articles concentrate on justifying cyberspace as an extension or a continuation of the real world.[28] [29] Such arguments can overstate the importance of formal black letter law. As a consequence of our singular focus on the design of the grand norms, more effective ways and means of regulation are neglected. The network society is a societal revolution; as such, it requires a new sociological understanding. Hence, a new foundation for regulation is needed, drawing on existing, albeit scant literature that both analyses the nature of the activities and the space in which they occur. Such an analysis will illustrate the inadequacies of traditional legal deterministic approaches and offer workable solutions to the problem of regulation and enforcement. [30]

Academics such as Murray and Biegel offer important perspectives on regulation of cybercrimes. [31] Murray points out that the regulatory models intervene to respond to a disruptive innovation, such as the internet. It is logical and necessary to incorporate arguments and experiences from cyberspace's normative and positive literature and experience into the debate over the regulation of cyberstalking. In the normative debate, according to cyber-libertarians, the appropriate regulatory regime for cyberspace is a system of self-governance in which users set the rules. [32] Skeptics, on the other hand, are critical of such a system. [33] They view it as anarchic and would apply existing law to cyberspace or introduce new laws to deal with undesirable behaviour. [34] Between these two extremes, a wide range of views has been expressed by Lessig and others. [35] For this reason, the article will consider whether methodologies offered by authors such as Murray and Biegel could be adopted to meet the particular challenges of cyberstalking. [36] [37]

Murray's analysis indicates that regulation of cyberspace would require identification of actors that are active within multi-level regulatory regimes. He constructed an abstract, a conceptually rich general-purpose illustrative matrix that depicts a three-dimensional regulatory field by means of points and lines representing regulatory modalities (regulators) and their protagonists or specific actions. [38] By contrast, Biegel was intent upon developing an all-encompassing regulatory model with the ability to address the majority of problems encountered in cyberspace. [39] Biegel applied his evidence to construct a five-step analysis, pointing whenever possible toward a combination of realistic approaches while trying in general to avoid major changes in the regulatory structure. [40] Law and code are the two principal means by which regulation should occur, according to Biegel. Although these approaches are vastly different, they all recognize that there is a need for restructuring of the regulatory mechanisms. Whatever form is adopted by the regulatory regime, its structure will always reflect the tension that exists between the need for flexibility and the equally compelling demand for consistency and predictability. [41]

2. Beneath a new dominion: Virtual Community

Is cyberspace subordinate to physical space, or is it separate from physical space? Is there a circular and productive relationship between cyberspace and physical space? McGuire argues that cyberspace is not distinct from physical space; it retains all the limited forms of spatial interaction at its core--while

simultaneously extending and complexifying them. [42] This can be demonstrated in various ways, including the visualisation of its structure, quantitative analysis, and the establishment of cyberspace geography. [43] [44]

What is striking about cyberspace is not only its omnipresence or ubiquity, but the sense of intimacy it creates. This entirely new social environment has creatively exploited the system's features so as to play with new forms of expressive communication, to explore possible public identities, to create otherwise unlikely relationships, and to establish behavioural norms. [45] [46] In so doing, cyberspace has invented new virtual communities and collaboratively constructed a sense of space and place. [47] [48] Although a considerable amount of research has been carried out to examine a wide variety of questions operating at various levels within the virtual community, few have successfully explored the link between virtual community and online behaviour.

What do we mean by virtual community? Traditionally, geography and emotional proximity have helped to indicate community. Geography arguably still remains important in defining virtual community, but we are better served in the Internet's context by an experiential conception of community rather than a geographic one. [49] Is the use of the phrase virtual community a perversion of the notion of community? In their seminal work, '*The Computer as a Communication Device'*, Licklider and Taylor explain why virtual communities most commonly consist of geographically separated members. They are communities not of common location, but of common interest. [50] Virtual community is defined by Rheingold as 'social aggregations that emerge from the Net when enough people carry on those public discussions long enough, with sufficient human feeling, to form webs of personal relationships in cyberspace'. [51] Interestingly, the technology of social networking was developed with a similar ideology, as Jonathan Abram's patent application to the US Patent and Trademark Office for Friendster explains:

> '… a system, method and apparatus for connecting users in an online computer system based on their relationships within social networks. The descriptive data and the relationship data are integrated and processed to reveal the series of social relationships connecting any two individuals within a social network'. [52]

A user of the system can determine the optimal relationship path (i.e., contact pathway) to reach desired individuals. Individuals in the system can be introduced (or introduce themselves) and initiate direct communication.

Not all scholars accept cyber subcultures as worthy of our attention, describing them as ephemeral, imagined communities, too fleeting, too superficial, and too virtual to warrant serious exploration. [53] They argue that cyber-libertarians have misunderstood the notion of a virtual community by overestimating the role of the disembodied individual, posting that the modern condition is one of indirect social relationships in which connectivity with others is more imagined, or para-social, than real. [54] Further, questions have also been raised as to how social relationships within a virtual community can be maintained in such a technological environment, where interactions among participants take place from a distance. [55] 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, cyberspace is merely developing categorical identities or imagined communities. Keleman and Smith define group interaction as occurring in one or many groups to which individuals belong at different points in time in order to ensure continuity in their social life. [56] These groups are constructed through individual engagement, and that is nothing more than the feeling of belonging to some group. In other words, it is a subjective perception and it does not exist independently.

However, there is an argument that virtual community as a concept is still amorphous due to a lack of shared mental models about what exactly constitutes community in cyberspace. [57] A more fitting abstraction is found in Oldenburg's 'The Great Good Places'. [58] The book theorizes that online communities may fill the desire for closeness associated with *gemeinschaft*, or unity of will. Such social bonding has been all but abandoned in many modern societies, where the social disconnect of *gesellschaft*, or the dominance of self-interest, has firmly taken hold. [59] Wall offers a particularly useful synthesis of these different thought streams, noting that virtual relationships contain neither the full panoply of social relationships nor the cohesive or organic expectations of *gemeinschaft*. [60]

So is there something disturbing about finding community through a computer screen? While analysts such as Williams and Boellstorff would answer this question in the positive, this paper proposes that computer simulation, at its core, is a tool of exploration. [61] [62] Many analysts speak of the closeness and trust borne

of these mediated connections using terms such as pseudo-*gemeinschaft*, virtual intimacy, or imagined community. [63] [64][65] Such designations reify the notion that interactions void of a face-to-face connection are somehow less than the real thing. However, according to Williams, non-face-to-face communication is not necessarily absent of presence. [66] In the virtual environment, users continue to host activity even when they log out. This characteristic, Boellstorff argues, creates a persistent presence in the virtual world, particularly in the three-dimensional virtual environments [67], and the three dimensions contribute to the overall realism effect: communicative, anthropomorphic, and photographic realism. [68] [69] It is undeniable, at least since Rheingold's 'Virtual Community' that friendships in cyberspace, mediated by virtual networks, can be as deep and meaningful as those acted out face-to-face. [70]

Facebook is regarded by most users as a safe and trustworthy community, and this perception helps to explain the impressively detailed nature of profiles found on this popular site. [71] The participants in such groups collectively create cultural resources for the construction of members' identities, not through shared geographical location, nationality, or other demographics *per se* but through shared social, (virtual) material, and discursive practices. [72] Consistent with the foundational work of Rheingold, Castronova suggests that the virtual world can be independent. Given the dominance of synthetic world technology, entire societies can be replicated and can operate on separate but parallel planes. [73] If we accept these arguments, then interactions within cyberspace are considered by the participants to be real. Such a conclusion would mean that the motives and the nature of potential harm related to cyberstalking activities warrant serious consideration.ions within cyberspace are considered by the participants to be real, such a conclusion

3. Theorising Cyberstalking

There is no consistent definition of cyberstalking in law or research. [74] It comes close to being a contested concept, which means it has yet to 'receive systematic analysis against an appropriate theoretical framework'. [75]As explained in the introduction to this article, the author's working definition of cyberstalking is threatening behaviour or unwanted advances directed at another using electronic communications technology. One of the main contentions within the body of literature which addresses cyberstalking is that cyberstalking is simply an extension of stalking and that the Internet is simply being used as an additional tool for stalking by the offline stalker. [76]Many theorists support such a view, noting that online and offline stalking share several important characteristics, including the desire by the offender to assert control over the victim, and the only novelty is in the methodology to inflict the harm. [77] [78] Still, others hold the view that cyberstalking is a new form of criminal behaviour unrelated to offline stalking and that cyberstalking ought to be understood as a new variant of an existing pattern of criminal conduct. [79] However, cyberstalking exhibits both continuities as well as discontinuities when compared with its terrestrial counterpart. [80]

It is the view of this author that cyberstalking is not merely stalking using the Internet. There are qualitative differences between stalking in physical space and stalking in cyberspace. [81] The increasing legal attention to cybercrime has also necessitated the need to establish the differences between crimes in the physical world and cyber-world crimes. Wall has suggested what he labels as elimination test to define differing forms of cybercrimes. [82] [83] Using this test, he concludes that there are three types of cybercrimes. First are traditional crimes where the Internet is simply a tool to assist in the crime. [84] An example of this would be the use of email by those planning a robbery. Second are hybrid crimes where the Internet has opened up entirely new opportunities for existing criminal activities. [85] An example of a hybrid crime under Wall's formulation is trading in sexually explicit materials. Third are true cybercrimes, which are solely the product of the Internet and can only be perpetrated within cyberspace (e.g. spamming). [86] Using this analysis, cyberstalking would appear at first sight to be a hybrid crime. It does not produce a new crime but simply expands on already extant deviant possibilities. [87] However, the significant differences between offline and online stalking are such that this author is reluctant to describe cyberstalking as a mere variant of physical stalking. [88] The use of the term hybrid may have a diluting effect the true characteristics and effects of this activity and, as a result, lead to the misinterpretation of its consequences. [89]

4. A Pragmatic Concept of Regulation

The question of whether the real-world notion of stalking will be applied to cyberstalking is still unresolved. Further, how should the law deal with virtual-related legal issues, such as stalking of a virtual individual? It has been established that the legal system is ill-equipped to deal with the issue of virtual crimes committed

by virtual personae. [90] The nature of the community in cyberspace and those who populate it is fundamentally different from the physical world, such that the nature and form of any regulation should be different. It can be argued that the structure of cyberspace encourages stalking. However, it can also be argued that merely having the ability to do something does not necessarily motivate a person to carry out that action. The law of our physical world is written to punish tangible crimes committed by real people, not virtual crimes acted out by online representations of self. Cyberstalking does not always conform to the reason and logic of the real world; hence, the law must treat cyberstalking activities differently than physical stalking. [91]

4.1 Is Cyberstalking Regulation Failing?

There is evidence to suggest that existing law is effective only where perpetrators can be identified, as, for example, where harassment law is sufficiently textured to deal with the nuances of cyberspace. [92] But can provisions designed for the physical world simply be transplanted into cyberspace? Is cyberstalking similar to or different from, say, negligent misstatement, where in *Patchett v Swimming Pool & Allied Trades Association Ltd,* Lord Justice Scott Baker stated:

> 'I agree that this appeal should be dismissed for the reasons given by the Master of the Rolls. I too would like to emphasise that no different legal principles apply to misrepresentations on a website than to those anywhere else in the public domain.' [93]

In many respects, there are significant differences between stalking and cyberstalking. As a result, the legal principles related to stalking should not be applied to cyberstalking. First, cyberspace can promote a false sense of intimacy and misunderstanding of intentions. [94] [95] In the absence of a real person and the sensory-perceptual stimuli that physical presence creates, a cyber-fantasy can be more easily expanded to meet the needs or desires of a stalker. [96] The limited nonverbal, historical and contextual information available in mediated contexts may encourage a potential cyberstalker to develop idealized perceptions of individuals and misjudge the intentions of the messages received from them. [97] In addition, the ease of use and the non-confrontational, impersonal, and sometimes anonymous nature of Internet communications may remove disincentives to cyberstalking. [98] The fusion of deviance and controls results in a new geometry of harm, where a potential stalker who may be unwilling or unable to confront a victim in person or on the telephone may show little hesitation to dispense harm remotely by sending harassing or threatening electronic communications to a victim. [99]

This lack of knowledge means that the harm suffered by victims of cyberstalking is often dismissed. [100] 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. [101] But in cyberspace, it is well known that people engage in anti-normative behaviour. [102] The loss of restraints can lead people to behave less altruistically; they feel less inhibited, express themselves more openly. [103] The temptation to engage in otherwise reckless, impulsive and disinhibited behaviour increases the probability of cyberstalking. It even provides the cyber-stalker with opportunity to enlist third-party participation, and the ensuing behaviours of third parties aggravate the intensity of suffering for the victim. [104] A victim usually has only the words of the offender to interpret online.

The second area of difference surrounds the relationship of stalker and victim. [105] In the physical world, an individual's ability to gather information is usually limited to celebrities, prior relationships, and those living nearby.[106] However, the nature of the Internet and the proximity (electronic propinquity) it creates make it possible for cyberstalking to be committed by strangers. [107] Often the online victim is unable to understand the lure of almost instant intimacy that the Internet offers, where a shy, troubled person may find it easy to share his pain with a faceless listener. Such an effortless and false sense of rapid intimacy can be very seductive, and this leads to a qualitative difference between offline and online stalking. [108] Alexy *et el* found that the perpetrators of cyberstalking were significantly more likely to threaten to kill themselves than the perpetrators of stalking. [109] This suggests that the cyberstalking perpetrator engages in more dramatic or histrionic behaviour.

The third difference surrounds the nature of the acts. Cyber-stalkers tend to concentrate on activities that are different from the activities of physical stalkers. Cyberspace provides the offender with the opportunity to monitor potential or existing victims on several levels, ranging from participating in a discussion forum and

becoming familiar with the other participants to searching the Internet for related information about an individual to accessing a potential victim's personal computer to gain additional information. [110] Although surreptitiously monitoring a victim while he or she is online increases the risk of detection and apprehension, it gives the cyberstalker more information about and contact with the victim and can fuel voyeuristic fantasies and feed an offender's need for a feeling of power over the victim. Such monitoring is possible in the physical world but can be a high-risk behaviour for the offender, whereas monitoring someone on the Internet is a comparatively low-risk activity. [111] In addition to the physical distance between a victim and an offender, few victims have the technical sophistication to determine that an offender is monitoring their activities. In this regard, cyberstalking is conceptually and empirically distinct from stalking.

Cyberstalking incidences are probably greater in number than claimed by law enforcement agencies, the media, or critics, and incidents of cyberstalking have increased enormously in the past few years. Although there are no studies that accurately document the extent of cyberstalking, this fact can be illustrated by the increasing number of reports related to online harassment [112]. 'Working to Halt Online Abuse' reports that it receives approximately *50-75 cases per week* for guidance and support to stop cyberstalking. [113] Additionally, the results of three pilot studies that focused on developing and refining a measure of cyberstalking victimization and the incidence of such victimization were analysed by Spitzberg and Hoobler. [114] Based on responses from 235 undergraduate communication college students, the study found that almost one-third reported some form of computer-based unwanted pursuit. [115]

There is a limited amount of UK-based research on cyberstalking, including its prevalence; however, individual case studies can be identified through the news media. The recently published ECHO pilot survey indicates that cyberstalking is occurring in the UK in ways which mirror international examples. [116] Unlike other areas within criminology that have an extensive historical precedent and a more visible impact, the majority of cyberstalking scholarship is not supported by empirical research. [117] Hence, both quantitative and qualitative studies are needed to improve our understanding of cyberstalking. There is a particularly strong need for studies of incidence data, documentation of the types and frequency of cyberstalking behaviours, examination of the relationship between physical or offline stalking and cyberstalking, development of cyberstalkers' profiles and histories, and outcome studies related to intervention strategies that support victims and eliminate or reduce cyberstalking.

Brenner argues that 'cyberstalking 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* and*mens rea*'. [118] Hence, for legal protections against cyberstalking to be effective, they must address the social and policy issues, along with the challenges to enforcement found in detection, identification, evidence gathering, attribution and jurisdiction. [119] This analysis stems from the assumption that the activity has been criminalised and that regulation will be imposed exclusively through laws. As a consequence of accepting this truth, the presumption is that cyberspace has rekindled the debate between regulatory forms, often encapsulated in the terms 'East Coast model,' here regulators rely on traditional legal command control techniques and 'West Coast model,' where regulators rely entirely on technology. [120] It is not obvious that either form of regulatory regime is appropriate, nor is it obvious how formal these legal identities are at present. [121] Today, we are not yet faced with parallel universes as developed in the 'Matrix', yet we are increasingly preoccupied with the virtual realities we now experience. [122] Certainly aspects of cyberspace are imaginary, but it is very real in terms of the consequences faced by participants who inhabit that space. [123] What would be the place of traditional defences and sanctions in this scenario? To which legal entity go the duties of regulation and liability?

Political reactions to this situation often jump at measures aimed 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 argues is based upon the categorisation of an individual to determine the acceptability of membership in certain social groups. [124] The imaginary character and life of the victim has that social identity merely by association with a community that exists in cyberspace.

It is also the very anonymity of the Internet that raises the question of what constitutes normal and deviant behaviours. [125] In a society dominated by the social norms that protect social identity, any behaviour that infringes upon the norm is deviant and therefore open to sanctions. The key is to allow for the unmasking of anonymous members when they engage in harmful activities. This, however, would require a significant modification of law enforcement methods for surveillance and investigation.

4.2 Regulation

One important question for regulation of cyberstalking is the distinction between what behaviour should be sanctioned, versus who should be responsible for investigating and imposing sanctions. Given the nature of cyberspace, concentration on enforcement is futile. Some believe that laws will only be obeyed if they are seen to be valid laws, where the provisions are well defined and justifiable and are derived from a legitimate authority.[126] How effective are laws adapted from those primarily designed to deal with harassment and physical stalking? Successful laws typically reinforce developing norms or expound on existing norms, clarifying uncertainties as they are developed. [127] Harassment laws provide for some recourse, but they are characterised by complexity due to the number of statutes that can be used to prosecute an offender. In the United Kingdom applicable laws are the*Protection from Harassment Act 1997;* the *Malicious Communications Act 1988, as extended by the Criminal Justice and Police Act 2001,* to include electronic communications; and relevant provisions of the *Computer Misuse Act 1990.* [128]

Since coming into force in the United Kingdom, the *Protection from Harassment Act 1997* (hereafter 'PHA 1977'), has been expanded significantly by the courts and is now considered by some to be one of the most widely framed piece of legislation enacted in recent years, extending well beyond its original intention of dealing predominantly with the issue of stalking. [129] However, this legislation is generally regarded as too general in nature. In reality, PHA 1997 has proven to be rather cumbersome and unwieldy for a rapidly changing online world. [130] As a result, the courts have recently attempted to rein in the breadth of the Act. In *Majrowski v Guys & St Thomas NHS Trust*, the House of Lords emphasised the difference between oppressive, unacceptable conduct and everyday irritations. [131] [132]

In contrast to the PHA 1977*,* where there is no minimum bar set for the nature of the conduct, the *actus reus* in the *Malicious Communications Act* 1998, is much narrower, requiring the perpetrator to display a 'credible threat'. It excludes less egregious behaviour on community-based cites such as Facebook, such as poking, tagging, repeatedly sending friend requests, or inviting others to join an application. Cumulatively, this conduct might cause annoyance or even distress, but it cannot be said to be indecent, grossly offensive, or threatening in nature. The subjective intent of the person can be difficult to prove. Arguably, this prevents innocuous comments from becoming the basis for legal proceedings. While it seems possible to adopt existing law where damage has been suffered purely by an offline person, it would be difficult to extend existing law to new victims whose existence as it relates to the offence is exclusively in cyberspace. It also ignores the fact that cyberstalking encompasses a wide range of new behaviours that are not associated with offline stalking. [133]

In the European context, stalking is still not viewed as a problem that must be systematically tackled. The Modena report, published in 2007, analysed the legislative framework on stalking across the European member states.[134] The report highlights that only 13 out of the 25 European countries have a specific law against stalking. [135] However, what this study underscores most forcefully is the apparent inconsistency in the provisions of existing legislation. Some legislation emphasises the reaction of the victim; other legislation seems to focus on the stalker's conduct and his/her intentions. Perhaps it is not surprising that variations also exist among those countries that have not enacted anti-stalking legislation. Half of these countries indicated that they felt the need to pass such legislation, but the other half did not think it was necessary, as they were satisfied with the existing legislation and/or prevailing society did not perceive stalking as a problem. [136] [137].

In the United States, both individual states and the federal government have adopted laws attempting to respond to perceived problems with cyberstalking. [138] However, recent statistics from 'Working to Halt Online Abuse' suggest that these laws have not yet proven effective. [139] The wider problem with existing legislation and other legal protections is that the remedies available are often not suited to the type of harassment experienced by online users, often conflicting with established cyberspace norms, and failing to curb the behaviour of wayward cyberspace users. [140] These cyberspace norms are developed by consensus among the entire body of cyberspace users, not those of the minority. [141] Cyberspace places limits on the use of law to control behaviour, but in order to have an effective method of regulation, it is not always necessary to intercede with legislation that is presented as the only viable solution.

When looking at the differences between physical stalking and cyberstalking, the character of cyberspace and its effects on social interactions, the nature of social ties, and the scope of experience and reality, Basu and Jones objected to regulation that, when implemented, would not only regulate deviant behaviour but would also criminalise some forms of legitimate behaviour. [142] Similarly in relation to the imposition of

intellectual property rules in cyberspace, Andersen argues that it would have been quite 'daft' if government had created obstacles to entrepreneurs innovating in railways and trains, simply to protect stakeholders in canals and barges and then criminalized the users of these services. [143] In the same context Bowery also comments, '…a law free sign still has some currency in it'. [144] Law only serves the purpose up to a point, and sometimes formal rules and regulations can produce policies that fail to take into account changing circumstances and that are highly unpopular.

In an attempt to propose an opposing school of thought, Salter and Bryden have argued for the creation of a new type of proscriptive orders, which they refer to as 'Internet Abuse Order.' [145] [146] The proposal, assumes the willingness of ISPs to act as enforcers by providing facilities to identify perpetrators and then sanctioning those persons. Why is this problematic so far as enforcement is concerned? It seems that Salter and Bryden have completely overlooked the fact that as a system of control, law must work mainly through deterrence, and 'Internet Abuse Order' would fail to act as a deterrent. [147] The problem is further escalated because frequently cyberstalking is committed by absolute strangers operating across multiple countries, which raises the issue of conflicting procedural requirements. More specifically, which nation has jurisdiction over the cyberstalker? It is also unclear how many nations have adequate laws for prosecuting cyberstalking. [148] Hence, the enactment of laws may be regarded as meaningless if individuals are uncertain or unaware that such legislation applies to them. [149]

By concentrating on enforcement rather than the substance of the rules, Salter and Bryden's proposal ignores the fact that in cyberspace, it is not always possible to identify the individuals whose behaviour contravenes the rules. At times it is even more problematic to determine the type of conduct that should be regarded as criminal. In such situation it may seem that a criminal prosecution would be counterproductive in a given instance that a case can be established beyond reasonable doubt, particularly with respect to the necessary intention to commit the relevant crime. The proposal is fundamentally flawed because compliance would be unfeasibly burdensome and expensive, would act as a coercive system by imposing liability on ISPs. It is not the legislation which is exclusively at fault. The problem lies with the enforcement of laws in a difficult environment, and the issues are about the existence of virtual communities, the anonymity of users, and the looming questions surrounding jurisdiction. [150] It is not about what law ought to be but, rather, what law is and how best to use it. [151] The enactment of new laws or the amendment of existing laws that allow for a more multi-faceted approach to the regulation of cyberspace should be considered. [152]

4.3 Regulatory Mechanisms

In their models for new regulation, Murray and Biegel explore the existing methodology for regulation of cyberspace. [153] [154] Murray's regulation form draws lessons from both the cyberlibertarian and cyberpaternalist camps. He argues that the regulatory matrix is a dynamic structure and that lawmakers should eschew the static approach and expands on a smarter, more dynamic regulatory model. [155] Further, it is argued that regulatory uncertainty creates a vacuum that traditional regulators rush to fill through command and control techniques. [156] Murray's approach, however, fails to offer a concrete roadmap to regulators, and it is also devoid of supportive theoretical arguments for implementation. In cyberspace, regulators and regulatees mingle with each other to such an unheard-of extent that regulatory interventions cannot be effective unless regulatees actively cooperate. [157] Indeed, the most effective in-world governance methods appear to involve proximal techniques, such as in-group reputation or shame-management strategies, rather than distal or external policing and criminal justice interventions. [158] While many may object, arguing that personal protection strategies are an infringement upon people's right to travel freely in cyberspace, such personal prevention strategies are employed on a daily basis in the physical world. The cyber-world is no different in its need for such safeguards.

The wholesale abandonment of conventional regulation or jurisprudence is not supported by Biegel. Instead, he encourages the application of lessons gained from prior analog problems to the challenges faced in cyberspace.[159] Three basic regulatory models, national law, international law, and code, are catalogued by Biegel. Based on his categorisation of allegedly problematic conduct, [160] Biegel has developed the analytic framework for a regulatory response which is comprised of five interrelated parts. [161] Included within his framework is a search for consensus. For the regulations to be effective, this consensus is necessary both at the rule-generating stage and at the enforcement stage. If it cannot be established that consensus is possible at these stages, then insurmountable problems are likely to persist, according to Biegel. [162] More specifically, Biegel implies that where there is no consensus, regulation via any of the three basic regulatory

models (or a combination thereof) will probably fail. As a result, any solutions generated by the framework must wait for favourable public consensus if those solutions are to be successfully implemented.

The problem with Biegel's model lies with his conviction that a single structure within one comprehensive set of rules is at all possible. In my view, his framework is overly broad. [163] Even though he suggests that each category of problems would have a corresponding category of similar solutions, he is resigned to the idea that some combination of all three regulatory models might work best for each activity in a given category. [164] To some degree, this argument undermines his argument for the categorisation of problems and the creation of category-based solutions. Biegel's model also fails to address the normative challenges and acceptability challenges inherent in such a regulatory approach, concentrating only on the feasibility challenges.

Are we, as Brenner suggests, merely tinkering at the edges of the problem of regulation? [165] The nature of regulation depends upon the categorisation of a crime, and for Wall, a clear distinction must be made between pure and hybrid cybercrime. Pure cybercrime, asserts Brenner, requires some combination of private legal action and technology, or as he describes it, 'a digital realist approach'. [166] This would lead us to subcategorise cyberstalking in order to differentiate between a 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 cyberstalking, where the victim and stalker may be hidden in pseudo characters within a virtual world far removed from reality. Although there appears to be little to prevent hybrid stalking from being rightly brought under existing criminal laws (essentially, stalking with refined tools), it would be equally wrong to simply expand existing legislation to cover pure cyberstalking.

Wall's argument that cyberstalking can be considered both as a hybrid and as a pure cybercrime is not being challenged. The point is not to engage in academic wrangling over exactly how Murray, Biegel or Wall has conceived this resistance of contradictory forms. It is arguably more worthwhile to develop a process through which cyberstalking should be addressed in the future. The nature of the activity and the virtual community in which it takes place require a more radical review of the issues. We cannot merely fall back on existing legislative or technological solutions. As Basu and Jones successfully argue, the question comes down to the perceived need to regulate this particular behaviour, cyberstalking, in cyberspace. [167]

The type of regulation to which one is attracted is dependent upon many factors. Legislators and writers steeped in the rule of law see the only solution in some form of regulation that is based upon legal identities. [168] Fixed within the physical world, imposed, formal and bureaucratic regulation is a given, top-down and rule-bound. This need not be the case. Communities and activities thrive both within and without formal regulatory mechanisms.[169] Conclusions from the Yahoo case [170] suggest the blurring between regulators and regulates in Cyberspace, it was the virtual communities, rather than government intervention, that forced the hand of Yahoo. Hence, the main focus should be on the development of a model for understanding how cyberspace can be socially controlled, taking into account aspects of formality/informality, visibility/invisibility, and the nature and extent of reactivity to deviant behaviours. [171]

4.4 Virtual Community as Opportunity: Use of 'Protocols'

Legal systems do not always provide consistent and predictable solutions to perceived societal problems. [172] It is my assertion that cyberspace has stretched the applicability of law-based regulation beyond the breaking point and that regulators have attempted to impose upon virtual communities and the often anonymous actors who populate them a formal, one-size-fits-all form of regulation that seems implausible. Laws do not automatically establish norms. Most virtual communities have already established norms to govern behaviour. [173] If new laws are created to regulate virtual communities and these laws are in conflict with established norms, the net effect is that the new laws will likely be disregarded. [174]

The vast majority of users in cyberspace act lawfully. How do we ensure that they continue to do so? Almost a decade ago, Lessig stated, '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.' [175] One approach would be to create an international organization of governments to enforce a common set of rules in cyberspace; however, one obvious problem with this method is that governments may not agree on what the rules should be.

Hence, the central question is how to create effective regulation that ensures control over only the deviant behaviour of the individual in the virtual community. Durkheim argued that deviant behaviour is 'an integral

part of all healthy societies' as opposition to deviant behaviour create opportunities for cooperation essential to survival of any group. [176]It is necessary to have mechanisms of social control, or a way of directing or influencing members' behaviour to conform to the group's values and norms. In order to solve the perceived problem of choice of law in cyberspace, we should concentrate on designing a smart system of regulation that can ensure flexibility, accountability and speed in deliberation. We need a set of rules that are more easily renewable and valid in more restrictive contexts. [177] These rules, termed 'protocols,' are declarations of best practices developed through experience and experimentation. [178] They represent a voluntary system of regulation based on mutual recognition of established norms in a virtual community. They are articulated and negotiated as codes of ethical conduct that individuals within a virtual community would presumably follow rationally rather than capriciously. [179] [180] Based on the principle that criminal law punishes offences against the 'collective conscience', these protocols would prescribe modes of conduct by emphasising or normalising particular forms of engagement. [181] They could be used to develop benchmarks and best practices that promote regulatory and enforcement strategies moving forward. The virtual communities have much to gain by developing provisions that would clearly define the scope of what is and is not permissible within the community.

A key distinguishing characteristic of protocols is that they are initiated by an individual decision to behave in particular ways within the virtual community, which creates expectations for others who observe this behaviour and feel compelled to emulate it. [182] In other words, protocols would evolve spontaneously from the bottom up rather than being intentionally imposed through legislation, and they would be voluntarily accepted by participants in the virtual community. An important aspect of this method of regulation is the concept of 'shared contexts,' in which people interact on common ground, and relationships among participants are not dependent on long-term sustainability or direct, personal interaction. In other words, context and content (or activities) are directly connected. Such a system would work particularly well in regulating cyberstalking and sociopathic behaviour associated with social networking platforms. The rules are valid only during the process. When the process is over, the rules are no longer valid. Typically, this is the difference between norms created by the cyberspace community and those promulgated by governments: the former are valid only for people who comprise a self-restricting virtual community, whereas the latter are broader and more general in scope. This would work in principle because it would only control the deviant behaviour in cyberspace and would also persuade human actors to behave in a desired manner by properly assessing the context of a situation. In an ideal situation, it would ensure that such protocols are spread through virtual communities by sharing. For example, if one virtual community is recognized as providing effective protection, other virtual communities should be able to use those protocols as a benchmark. Although this effect is not assured, protocols over time do have the capacity to influence change in ways that differ from laws promulgated by governments. [183]

Because these protocols, or rules, would not be bound to any existing law, they would be more flexible and adaptable in nature and would have a sense of universality about them. For instance, if conditions change and the community decides that for their purposes, behaviour that was attractive in the past has ceased to be useful, the community can voluntarily devise a new behavioural protocol. Thus, an existing norm can be quickly replaced by a new norm through simultaneous recognition of members of the virtual community. Hence, these protocols would have the ability to bring about change in ways that differ from the stringent legislative process.

The development of such protocols would seek to shift the focus from the creation of restrictions to the protection of unique interests and concerns of individual virtual communities. [184] The task is one of showing how the protocols could be reconciled with the formal categories of the law. Berman's reasoning of *lex mercatoria* recognises that law does not reside exclusively with a sovereign power; rather, law is constantly evolving through the contest of various norm-generating communities. [185] Hence, protocols as law will be required to supplement regulation if weak parties are to be effectively protected. In other words, because cyberspace has an individualistic feature and is difficult to regulate in terms of the legal tradition (norms - norms violation - coercion), protocols based upon mutual respect that follow the values of the consent of the governed and that are fashioned to address a virtual community's autonomy are likely to prove effective. [186]

Earlier in this paper, I highlighted a number of unique and at times interrelated challenges, including the problem of anonymity, jurisdictional issues, and lack of resources or expertise law enforcement authorities face when attempting to investigate and prosecute cyberstalker. Would protocols work to regulate cyberstalking in such instances? In theory, they can. To some degree such mechanisms already exist, although they are rather peripheral in their current form. For example, one of the major problems with

cyberstalking, as stated previously, is underreporting. Victims often feel that the behaviour is not serious enough to warrant the attention of the police, or they do not believe that law enforcement agencies will take the matter seriously. [187] It is my argument that once protocols are developed and put into place, they will help to reduce indifference by increasing the prospects for reciprocal awareness. Yet another problem faced by law enforcement is related to the legitimacy of laws in a cross-jurisdictional context. Protocols can actively stave off crises of legitimacy because they are not tied to any particular jurisdiction.

What if 'cyber-socialisation' in virtual communities results in cyberstalking? In response to this, I argue that within virtual communities, regulation of deviant behaviour has matured rapidly in recent years, evolving largely from a vigilante movement into a formal policing model. [188] As individuals within a virtual community cooperatively engage in successful bilateral relationships to follow established protocols, others are likely to notice their cooperative behaviour and attempt to initiate mutually beneficial relationships with them. [189] It is probable that once a general level of compliance is achieved, an obligation would be created that ensures all members obey those rules for the common good of the community.

How would the virtual community respond to an individual who decides to violate the protocols? Any deviant behaviour which undermines the protocols would be seen as an offence to the 'collective sentiments' because it threatens the virtual community as a social institution. This would entitle the virtual community to impose sanctions. However the decision to impose sanctions can be taken only by the virtual community as an arbiter through 'positive consensus'. [190] Importantly, however, when information spreads about deviant behaviour of a particular individual, all of the beneficial relationships that the individual enjoys within the virtual community should rightfully be placed in risk. [191] Hence protocols will enable the community members to go far beyond than establishing a norm; it would be able to mount interventions in governance of the virtual community.

In other words, the protocols should act as enforcers of a retributive form of morality, resulting in unconditional compliance with protocols when an individual chooses to enter into some form of interaction, along with a refusal to interact with any individual who is known to have adopted undesirable behaviour with anyone within the community. [192] This collective pressure to conform to protocols would dramatically increase their effectiveness as a deterrent, because non-conformity would put the individual at greater risk of isolation from the community. [193] Thus, a community member's reputation serves as a bond that will be forfeited if one is not reliable. [194]

The confrontation between societal freedoms and individual safety is frequently highlighted in debates surrounding virtual communities. We have seen that the illegal status of so-called unacceptable behaviour associated with cyberstalking may well rest primarily on laws that do not directly address the perceived crime. For instance, in the U.S. case of Megan Meier, who committed suicide when an adult neighbour harassed her online, the neighbour was prosecuted on 'accessing protected computers without authorization' and one count of conspiracy, not the act of harassment itself. [195] This ruling was overturned because it was deemed to criminalise anyone who signed up for an online service using inaccurate or fake information, a common online practice. [196] However, through the establishment of protocols, it is possible to impose a moral obligation on individuals, virtual communities and other service providers who are responsible for monitoring behaviour. [197] In the absence of the social pressures of inappropriateness, it is difficult for people to evaluate others and adjust their performance according to the values, context and perceptions of the entire virtual community. Arguably, the moral conscience of the virtual community is a more effective deterrent against deviant conduct than traditional governance (proximal or distal). [198] However, if sanctions are necessary, they should be based upon the degree of severity of the violation: for example, applying peer pressure versus expulsion. The community is indeed a powerful force in cyberspace and in certain situations. As such, social norms identified by a virtual community are not easily disregarded. [199] Importantly, such protocols must be disseminated among all members of a virtual community, and their use must be strongly encouraged in order to ensure the efficacy of a system of oversight.

4.5 'When Protocols Fail'

Although this analysis is generally correct in so far as the question it seeks to answer, it is crucial to understand that the effectiveness of protocols will be limited to cyberstalking which takes place within a virtual community. They are designed to maintain the internal order of a virtual community. It is acknowledged that there may be problems of unpredictability regarding acceptance among the early adopters, as potentially there may be a gap between what the protocols should enforce and what they are actually expected to enforce.

The protocols and the philosophical underpinning become dysfunctional when the 'collective sentiments' are involved with the deviant activities or the members might well prefer a lawless virtual community. [200] [201] [202]This creates problems in deciding what to enforce and whom to punish. In such situations, a 'continuum of regulation' [203] is required as protocols would lose the power to control behaviour; what stops delinquency is the formal law that imposes responsibilities upon the virtual communities to provide protection of social and moral norms. [204] Importantly, control that is external to the virtual community is enforced through the use of formal sanctions as deviance develops into a crime. [205] Here, formal law offers corrective actions through its values and estimation of human rights.

Furthermore, practical constraints may limit the enforcement of sanctions because in cyberspace it is possible for a user to assume multiple identities. In Ellickson's example of Shasta County, the norms were successful in regulating the behaviour of the cattle farmers because each resident possessed only one unchanging identity that they wanted to protect; the owner of trespassing cattle would be known to all of the residents by name and appearance, making him recognisable and therefore unable to escape from blame and countermeasures in future encounters. [206] In order to overcome this, users could be prevented from creating more than one account. However, this could result in fewer people joining the community, or users could circumvent this safeguard by registering with different email addresses. [207] This would further complicate the enforcement analysis. However, I argue that by implementing a reputation analysis mechanism, similar to that of eBay, [208] along with the sanctions, it is possible that the number of deviant acts would decline, as would the number of virtual identities created by one user. [209] [210] However, what happens when such a system fails? eBay 'quickly learned that to prevent fraud, enforce its contracts, and ensure stability in its auction services, it would depend critically on government coercion and the rule of law.' [211] But even then, we must find a more principled method of applying laws to deviant behaviour within the virtual communities. As Dibbell argues, 'considering the novelty of this realm, we might reasonably hope for future case law and legislation to do a better job of it, but I suspect it will be a long time before enough of those ambiguities are ironed out to make a difference.' [212]

One of the strange effects of protocols is a kind of fusion of three elements of law, namely: institutional, procedural and personal separation of law-making; law application; and law enforcement. [213] It is entirely plausible that this shortcoming of protocols may be exploited by an over-eager and over-vigilant community. [214] For example, community hysteria associated with false reports of abuse may result in discrimination against targeted individuals by the employment of coercive threats and by possible imposition of other rules which extend beyond the norms that community members are expected to follow. [215] Further heterogeneity of interests could also create problems with the application of protocols. Since individuals are exposed to different influences and circumstances, it is inevitable that not all members of a virtual community will be equally committed to the 'collective sentiments.' As the size of a community increases, it becomes less likely that all of its members will share a commonality of interests. Members may begin to feel anonymous, and therefore may feel less socially constrained in their actions. [216] There may also be conflicting interests and problems of trust between the members of the community. [217] This is particularly likely to occur when incentives are asymmetrically distributed in the community. In such a situation, the protocols may be used to address conflict by carefully balancing the interests of the individual against the interests of the community, but this will not always eliminate conflict. [218] The protocols may precipitate superior bargaining power for the prevailing side, collective action problems for dissenters, or the use of strategic behaviour by both sides.

In addition, a common objection to a voluntary system of regulation is the perceived problem of enforceability in the absence of outside persuasion. [219] It is accepted that enforceability of protocols would be completely dependent on social sanctions whose legitimacy is derived from the endorsement of the members of the virtual community. [220] This means that protocols are 'enforced' only to the extent that community members respect them. [221] One potential problem may be that the only members of the virtual community who respect the protocols probably would not be the ones responsible for the deviant behaviour in the first place.

Such an objection ignores the efficacy of the threat of various sanctions by other group members, which would greatly contribute to the normal functioning of virtual communities.

5. Conclusion: A Choice between 'No Solution' and 'Compromise'

> *You never change things by fighting the existing reality. To change something, build a new model that makes the existing model obsolete*
>
> *-- R. Buckminster Fuller*

In recent years, a succession of legal articles proposing regulation of cyberstalking have either attempted to justify cyberstalking as an extension/continuation of stalking or have overemphasised the importance of formal black letter law. They have rarely looked into cyberspace with any real social insight, instead focusing on the question of how to adapt laws of the real world for application in cyberspace. Cyberstalking, however, does not always conform to the reason and logic of the real world. Although cyberstalking exhibits both continuities as well as discontinuities, I have critically argued for a new variant of an existing pattern of criminal conduct, one that encompasses the *actus reus* and the *mens rea.* Hence, in order for regulation of cyberstalking to be effective, it must address social as well as policy issues, along with the challenges to enforcement found in detection, identification, evidence gathering, attribution and jurisdiction.

As this article has demonstrated, Web 2.0 represents a societal revolution; as such, regulation requires a sociological understanding of its structure and capabilities. What is striking about Web 2.0 is the sense of false intimacy it creates. This entirely new social environment has creatively exploited the system's features so as to play with new forms of expressive communication, to explore possible public identities, to create otherwise unlikely relationships, and to establish behavioural norms. In a way, the constructs of this environment have managed to create a stalker's paradise.

The central paradigm of this article argues that in order for regulation of cyberstalking to be effective, a more expansive view of regulation should be adopted by entrusting the choice of control to the virtual community. This places the role of regulating behaviour squarely on the shoulders of the virtual community, where it belongs. Based on the 'rights and responsibilities' discourse, the philosophical underpinning of protocols recognises the value of virtual community and aims to provide a novel solution to behavioural problems such as cyberstalking by balancing individual rights against communal norms. Although this focuses primarily on the regulation of cyberstalking in a social networking context, it may have much broader relevance and significance, e.g., when applied to cyber-bullying, cyber-harassment, and on-line deception offences, as many of the arguments made here could also be applicable in these wider offending contexts.

This article is intended to suggest an answer to the cognitive question of regulation of cyberstalking in Web 2.0, while also addressing the more intricate normative question related to the procedure for regulation. The optimal answers are not obvious, as the traditional approaches to legal regulations are based on the purported intrinsic rationality of social norms. The author, however, believes that control-dynamics of protocols provide a more realistic solution designed to make the best of a bad situation.

The spheres of regulation affecting cyberspace have developed rapidly in recent years, while the nature of regulation within cyberspace has simultaneously faced major challenges. The high cost of pursing criminals in cyberspace means that while many governments have laws mandating prosecution of many cyber-criminal activities, most of them have no significant law enforcement presence in cyberspace. As I have discussed before in this paper, the makers of policies and laws are seldom aware of the societal structure of cyberspace, and for this reason the laws they create often fail to achieve the desired level of enforcement. The problem with most of the legislation regulating cyberspace is that it is too sweeping in nature, and some of it is, in fact, poorly thought through, reactive legislation based on political aspirations, which almost always reflect conflicting efforts to achieve conflicting objectives. However, as argued before in the article, legislation is not the only method of social regulation; hence, it is not necessary for regulation in the future to come in the form of instruments made by or under a legislative body, because as a tool of control and deterrence, such instruments are substantially undermined in cyberspace. There simply would never be enough resources to detect and sanction the majority of deviant behaviour. In other words, the unavoidable reality is that the vast legal grey area that exists today also operates in favour of the cyberstalker.

Virtual communities can provide a sense of belonging and social identity to an individual. Protocols force us to examine virtual communities, both for the good they offer and the potential harm to members arising from abuses. Such a new and unique arrangement requires that we look to the structural social forces that shape communities and define their members. This focus on the common good invokes a communal obligation to prevent deviant behaviour within virtual communities. Although there can be disagreement on the question of whether protocols as extra-legal norms themselves are good or bad, and on the question of whether and how the law should take them into account, one cannot deny that hasty adoption of inflexible and possibly inappropriate new legislation will do more harm than good.

Because protocols are facilitative rather than prescriptive in nature, they offer an alternative to the parochial regulatory framework perpetuated by legislative bodies. The argument for applying protocols to promote law and order in a polycentric and purely voluntary setting within cyberspace is quite compelling, as there is another benefit as well: protocols are produced and supported by institutions (virtual communities), which are not attempting to monopolise law; hence, protocols provide a mechanism for avoiding the politicised laws of the nation states.

In many respects, the struggle over regulation demonstrates rather tellingly that we are ill-prepared for the psychological cyber-world we have created. Censoring social networking sites will do little to weed out the problem and may well block access to sites that are socially beneficial. I further argue that there is a need for a policy approach that better balances the protection of individuals and the successful development of social networking and virtual communities. If we upset this necessary balance, which I believe would be the case if we try to over-regulate and there is excessive government interference, then there will be less for everyone. By less for everyone, I mean reduced usefulness of virtual communities and an accompanying diminishment of their core purpose. It seems highly likely that the online environment will be left the poorer for it.

Protocols will coexist with law and may also influence relevant legislation, but they will not eliminate its necessity entirely. The interaction between community-based protocols and necessary laws is complex and has yet to be fully explored. It is my argument that the prospect of legal remedies should be invoked only when protocols are rendered ineffective. As previously discussed, a control model of legal authority to regulate cyberstalking is not only expensive and minimally effective, but also undermines forms of social capital that promote long-term user commitment to virtual communities. The exercise of authority through the application of protocols strengthens the social bond between individual users and the virtual community as a whole. Protocols that are based on social values and normative commitment promote compliance and cooperation, both of which are more stable and more sustainable in the long-run when arrived at by consensus. It is my belief, that the development of protocols represents a positive regulatory response, because such protocols would be attached to and would continue to evolve with the individual virtual communities they are designed to protect. Most certainly, the establishment of such protocols is an idea that is worthy of continued exploration and analysis.

---

[1] Subhajit Basu is Senior Lecturer in CyberLaw,School of Law, University of Leeds,
Email: s.basu@leeds.ac.uk

[2] See Home Office, *Stalking—the solutions: A consultation paper* (London: Stationery Office, 1996) 1.2

[3] Most policy discussions in this area are based upon one or more of the following sets of alternatives. The first alternative is whether our policies for cyberspace should depend on the market or the State. The second is whether these policies should favour ‘bottom-up’ or ‘top-down’ regulation. Occasionally, a third policy set is produced, which takes into consideration any other, more desirable approach apart from a formal legal response by the State.

[4] The article primarily focuses on cyberstalking in the Social Networking context, and the legal position in UK is used as point of reference. However, this article has potentially much broader relevance and significance e.g. to on-line deception offences; or the range of offences involving children as many of the arguments made here could also be relevant in these wider offending contexts.

[5] The principal proponent of ‘responsive communitarianism’ is Amitai Etzioni. Etzioni aims to solve societal problems by balancing individual rights with communal norms. See Etzioni, A., et al., ‘The *Responsive*

Communitarian Platform: Rights and Responsibilities', in Schumaker, P., (Ed.) *The Political Theory Reader* (MA: Wiley-Blackwell, 2010) 231

[6] 'Protocols' identified as such in this research article.

[7] See Bell, D., 'Communitarianism', in Zalta, E. N., (Ed.) *The Stanford Encyclopaedia of Philosophy* (Spring, 2005)

[8] The principal proponent of 'responsive communitarianism' is Amitai Etzioni. Etzioni aims to solve societal problems by balancing individual rights with communal norms. See Etzioni, A., et al., 'The *Responsive Communitarian* Platform: Rights and Responsibilities', in Schumaker, P., (Ed.) *The Political Theory Reader* (MA: Wiley-Blackwell, 2010) 231

[9] Based on the 'rights and responsibilities' discourse-the philosophical underpinning of protocols recognises the value of community, essentially the connection between an individual and community. It stresses upon the role of community in regulating behaviour. Etzioni, A.,(Ed.) *The Essential Communitarian Reader* (Maryland: Rowman & Littlefield, 1998); see Bell, D., 'Communitarianism' in Zalta, E. N., (Ed.) *The Stanford Encyclopaedia of Philosophy* (Spring, 2005); see also Etzioni, A., et al., 'The *Responsive Communitarian* Platform: Rights and Responsibilities', in Schumaker, P., (Ed.) *The Political Theory Reader* (MA: Wiley-Blackwell, 2010) 231

[10] Fafinski, S., Dutton, W.H., and Margetts, H., 'Mapping and Measuring Cybercrime' (2010) OII Forum Discussion, Paper No. 18 (Oxford Internet Institute, University of Oxford) 18

[11] Reed, C., *Making Laws for Cyberspace* (OUP, 2012)

[12] See Brenner, S. W*.,* 'Distributed Security: Moving Away from Reactive Law Enforcement' (2005) 9 *International Journal of Communications Law & Policy,* 1-43; see Wall, D., 'Digital Realism and the Governance of Spam as Cybercrime' (2005) 10 (4) *European Journal on Criminal Policy and Research*, 309-335; see also Deibert, R. J., and Rohozinski, R., 'Risking Security: Policies and Paradoxes of Cyberspace Security' (2012) 4 (1) *International Political Sociology*, 15–32

[13] Further, also linked to anonymity is the issue of identity in cyberspace and the related notion of the truth-lies dichotomy i.e. trust is built through virtual communication rather than face-to-face interaction. This completely alters the nature of the victim-offender relationship and makes it more difficult to regulate. See Whitty, M.T., and Johnson, A.N., *Truth, Lies and Trust on the Internet* (Hove and New York: Routledge, 2009)

[14] See White, B. A., *Second Life: A Guide to Your Virtual World* (QUE, 2007) 416

[15] Social relationships are turning into social capital, where the main objective is not to have but to do relationships. See Wittel, A., 'Toward a network sociality' (2001) 18 (6) *Theory, Culture & Society,*72*,* 51-76; see also Barfield, W., 'Intellectual Property Rights in Virtual Environments: considering the rights of owners, programmers and virtual avatars' (2006) 39 *Akron Law Review*, 649, 651

[16] Social relationships are turning into social capital, where the main objective is not to have but to do relationships. See Wittel, A., 'Toward a network sociality' (2001) 18 (6) *Theory, Culture & Society,*72*,* 51-76; see also Barfield, W., 'Intellectual Property Rights in Virtual Environments: considering the rights of owners, programmers and virtual avatars' (2006) 39 *Akron Law Review*, 649, 651

[17] Cooke, M., and Buckley, N., 'Web 2.0, Social Networks and the Future of Market Re-search' (2008) 50 (2) *International Journal of Market Research* , 267–292; see Greenfield, A., *Everyware* (New Riders: Berkeley, 2006); see also Hand, M., *Making Digital Cultures: Access, Interactivity, and Authenticity* (Hampshire: Ashgate, 2008) (discussing the implication of sharing personal information in social networks).

[18] The present generation (teenagers and twenty-something) 'far from valuing privacy and boundaries, like earlier generations, embody a new kind of self-obsessed broadcast culture'. Buss, A., and Strauss, N., *Online Communities Handbook: Building your Business and Brand on the Web* (Berkeley: New Riders, 2009) 31; see also Beck, U., and Beck-Gernsheim, E., *Individualization* (London: Sage, 2002)

[19] See McGrath, M. G., and Casey, E., 'Forensic Psychiatry and the Internet: Practical Perspectives on Sexual Predators and Obsessional Harassers in Cyberspace' (2002) 30 (1) *The Journal of the American Academy of Psychiatry and the Law*, 81–94

[20] 'A fully filled-out Facebook profile contains about forty pieces of recognizable personal information…. Facebook then offers multiple tools for users to search out and add potential contacts'; see Grimmelmann, J., 'Saving Facebook' (2009) 94 *Iowa Law Review*, 1149; see Li, C., and Bernoff, J., *Groundswell: Winning in a World Transformed by Social Technologies* (Boston: Harvard Business Press, 2008) (for a detail discussion on impact of social media and virtual communities on society); see also Qualman, E., *Socialnomics: How Social Media Transforms the Way We Live and Do Business* (Hoboken, N.J.: Wiley, 2009)

[21] See Ybarra, M. L., and Mitchell, K., 'How risky are social networking sites? A comparison of places online where youth sexual solicitation and harassment occurs'(2008) 121(2) *Pediatrics,* 350-357; see also Filosa, G., *Online profiles attracting sexual predators, feds warn; Teen sites being used as victim directories* (The Times- Picayune, 2007)

[22] 'Foursquare' uses a smartphone's global positioning system (GPS) to broadcast the precise location of the user to the 'friends' and, should the user wish, to the wider world. Users are encouraged to 'check in' on their phone whenever they arrive at a point of interest. An application like Foursquare or 'Google latitude' can be used to monitor user activity in an effort to build a rich database of personal information.

[23] 'Foursquare' uses a smartphone's global positioning system (GPS) to broadcast the precise location of the user to the 'friends' and, should the user wish, to the wider world. Users are encouraged to 'check in' on their phone whenever they arrive at a point of interest. An application like Foursquare or 'Google latitude' can be used to monitor user activity in an effort to build a rich database of personal information.

[24] Küpper, A., *Location-based services: fundamentals and operation* (Hoboken, NJ: John Wiley 2005)

[25] See Coates, J., Suzor, N., and Fitzgerald, A., ' *Legal aspects of web 2.0 activities: Management of legal risk associated with the use of YouTube, MySpace and Second Life'(*Brisbane: ARC Centre of Excellence for Creative Industries and Innovation and Queensland University of Technology, 2007)

[26] Demetriou, C., and Silke, A., 'A Criminological Internet 'Sting': Experimental Evidence of Illegal and Deviant Visits to a Website Trap' (2003) 43(1) *The British Journal of Criminology*, 213-222

[27] Another key variable related to the differences between inter-personal crimes in the real as well as in virtual world is that of victim vulnerability and accessibility. See Demetriou, C., and Silke, A., 'A Criminological Internet 'Sting': Experimental Evidence of Illegal and Deviant Visits to a Website Trap' (2003) 43(1) *The British Journal of Criminology*, 213-222. See also Ybarra, M. L., Mitchell, K., Finkelhor, D., and Wolak, J., 'Internet prevention messages: Are we targeting the right online behaviors?' (2007) 161 (2) *Archives of Pediatric and Adolescent Medicine,* 138–145

[28] See Salter, M., and Bryden, C., 'I can see you: harassment and stalking on the Internet' (2009) 18(2) *Information & Communications Technology Law*, 99-122; Chik, W., 'Harassment through the Digital Medium A Cross-Jurisdictional Comparative Analysis on the Law on Cyberstalking' (2008) 3(1) *Journal of International Commercial Law and Technology*, 13-44; see also Ogilvie, E., *Cyberstalking*, *Trends and Issues in Crime and Criminal Justice, No.*166 (Canberra: Australian Institute of Criminology, 2000)

[29] Several academics concerned with law and regulation of cyberspace has focused on the question, how to adapt laws of the real world to cyberspace. See Lastowka, G. F., and Hunter, D., 'Virtual crimes' (2004) 49(1)*New York Law School Law Review*, 293–316; see also Wall, D., and Williams, M., 'Policing diversity in the digital age: Maintaining order in virtual communities' (2007) 7 (4) *Criminology and Criminal Justice*, 391-415

[30] National regulation tends to fail due to implementation problems because of the transnational nature of cyberspace. In contrast, an internet specific regulation through legitimate international law-making also threatens to fail due to the difficulties in reaching intergovernmental consensus. Goldsmith, J., 'The Internet, Conflicts of Regulation and International Harmonization', in Engel, C., (Ed.) *Governance of Global Networks in the Light of Differing Local Values* (Baden-Baden, Nomos, 2000)

[31] See Murray, A. D., *The Regulation of Cyberspace* (Abingdon: Routledge-Cavendish, 2007); see also Biegel, S, Beyond *Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace*(Cambridge: Mass: MIT Press, 2003)

[32] See Johnson, D., and Post, D., 'Law and Borders--the Rise of Law in Cyberspace' (1996) 48 *Stanford Law Review*, 1368-1378; see Perritt, H. H. Jr., 'Cyberspace Self-Government: Town Hall Democracy or Rediscovered Royalism?' (1997) 12 (2) *Berkeley Technology Law Journal*, 413; see also Gibbons, L. J., 'No

Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace' (1997) 6 *Cornel Journal of Law and Public Policy*, 475

[33] See Goldsmith, J., 'Against Cyberanarchy' (1998) 65 (4) *University of Chicago Law Review* 1199; see Rothchild, J., 'Protecting the Digital Consumer: The Limits of Cyberspace Utopianism' (1999) 74 (3) *Indiana Law Journal,* 893; see also Wu, T.S., 'Cyberspace Sovereignty? The Internet and the International System' (1997) 10 (3) *Harvard Journal of Law and Technology*, 647; and also Goldsmith, J., and Wu, T.S., *Who Controls the internet: Illusions of a Borderless World* (OUP, 2006)

[34] See Wall, D., 'Digital Realism and the Governance of Spam as Cybercrime' (2005) 10 (4) *European Journal on Criminal Policy and Research*, 319, 309-335

[35] See Koops, Bert-Jaap., et al, *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-Liners* (The Hague: TMC Asser Press, 2006); see also Cairncross, F., *The Death of Distance: How the Communications Revolution will Change Our Lives* (Harvard Business Press,2001); Reidenberg, J. R., 'Governing Networks and Rule-Making in Cyberspace' (1996) 45 *Emory Law Journal*, 911; Murray, A.D., *The Regulation of Cyberspace* (Abingdon: Routledge-Cavendish, 2007)

[36] Murray, A. D., *The Regulation of Cyberspace* (Abingdon: Routledge-Cavendish, 2007)

[37] Biegel, S., *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace* (Cambridge: Mass: MIT Press, 2003) 220

[38] Murray, A. D., *The Regulation of Cyberspace* (Abingdon: Routledge-Cavendish, 2007) 54

[39] Koops, Bert-Jaap et al, *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-Liners* (The Hague: TMC Asser Press, 2006)

[40] Biegel, S., *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace* (Cambridge: Mass: MIT Press, 2003) 224-225

[41] Brownsword, R., *Rights, Regulation, and the Technological Revolution* (OUP, 2008) 287

[42] McGuire, M., *Hypercrime: The New Geometry of Harm* (London: Routledge-Cavendish, 2007) 7

[43] Huberman, B.A., and Adamic, L.A., 'Growth dynamics of the World-Wide Web' (1999) 406 *Nature*, 450-457

[44] Shiode, N., and Dodge, M., 'Spatial analysis on the connectivity of information space' (2000) 8(2) *Theory and Applications of GIS*, 17-24; see also Murnion, S., and Healey, R.G., 'Modelling distance decay effects in Web server information flows' (1998) 30 (4) *Geographical Analysis*, 285-303

[45] Yee, N., 'The Psychology of Massively Multi-User Online Role-Playing Games: Motivations, Emotional Investment, Relationships and Problematic Usage', in Schroeder, R., and Axelson, A., *Avatars at Work and Play: Collaboration and Interaction in Shared Virtual Environments* (Springer: Netherlands, 2006) 187-207

[46] See Miller, D., and Slater, D., *The Internet: An Ethnographic Approach* (Oxford: Berg, 2000). See also Halder, D., and Jaishankar, K., 'Online Social networking and Women Victims', in Jaishankar, K., (Ed.)*Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* (Boca Raton, FL: CRC Press, 2011) 301-320

[47] Reid, E., 'Virtual Worlds: Culture and Imagination', in Jones, S. G.,(Ed.) *Cyber society: Computer-Mediated Communication and Community* (London: Sage, 1995) 164-183

[48] See Moore, R., Ducheneaut, N., and Nickell, E., 'Leveraging virtual omniscience: Mixed methodologies for studying social life in persistent online worlds' (2005) Workshop presented at the Games, Learning, and Society Conference, Madison WI, June 23-24, 2005; see also Miller, D., and Slater, D., *The Internet: an Ethnographic Approach* (Oxford/New York: Berg, 2000)

[49] Alexander, G.S., 'Dilemmas of Group Autonomy: Residential Associations and Community' (1989) 75 (1) *Cornell Law Review*,17–33

[50] 'Geographically separate but intellectually proximate minds'; see Licklider, J. C. R., and Taylor, R. W., 'The computer as a communication device' *,* (1968) Science and Technology Republished in SRC Research Report 61, Digital Equipment Corporation, 1990, 37-38. Available at: //ftp.digital.com/pub/DEC/SRC/research-reports/SRC-061.pdf; see also Mayer-Schonberger, V., and Crowley, J., 'Napster's Second Life-The Regulatory Challenges of Virtual Worlds' (2006) 100 (4) *North Western University Law Review*, 1775, 1781

[51] Rheingold, H., *The virtual community: Homesteading on the electronic frontier* (Reading, MA: Addison-Wesley,1993) 5

[52] http://www.out-law.com/page-7092

[53] See Lockard, J., 'Progressive politics, electronic individualism and the myth of the virtual community', in D. Porter (Ed.) *Internet Culture* (New York: Routledge, 1997) 219-232; see also Healy, D., 'Cyberspace and place: The Internet as middle landscape on the electronic frontier', in Porter, 02D., (Ed.) *Internet Culture* (NY: Routledge, 1997) 55-68; early reactions from anthropologists also highlighted a sense of scepticism to 'continuous virtual experience', see Heim, M., *The Metaphysics of Virtual Reality* (Oxford: OUP, 1993); Boal, I.A., 'A flow of monsters: Luddism and virtual technologies', in Brook, J., and Boal, I. A., (Eds.) *Resistingthe Virtual Life: the Culture and Politics of Information* (San Francisco: City Lights, 1995) 3-15 0

[54] Calhoun, C., 'Indirect Relationships and Imagined Communities: Large-Scale Social Integration and the Transformation of Everyday Life', in Bourdieu, P., and Coleman, J. S., (Eds.) *Social Theory for a Changing Society* (San Francisco- Oxford: Boulder, 1991) 95-121

[55] Wall, D., and Williams, M., 'Policing diversity in the digital age: Maintaining order in virtual communities' (2007) 7 (4) *Criminology and Criminal Justice*, 393, 391-415

[56] Keleman, M., and Smith, W., 'Community and its 'virtual' promises, A critique of cyber libertarian rhetoric' (2001) 4 (3) *Information, Communication & Society*, 370-387

[57] Fernback, J., 'The Individual within the Collective: Virtual Ideology and Realisation of Collective Principles', in Jones, S., (Ed.) *Virtual Culture* (London: Sage Publications, 1997) 36–54

[58] See Oldenburg, R., *The Great Good Places* (NY: Paragon House,1989)

[59] Oldenburg, R., *The Great Good Places* (NY: Paragon House,1989)

[60] Wall, D., *Cybercrime: The Transformation of Crime in the Information Age* (Polity: Cambridge, 2007) 33

[61] Williams, M., *Virtually Criminal: Crime, Deviance and Regulation Online* (London: Routledge, 2006)

[62] Boellstorff T., *Coming of Age in Second Life: An Anthropologist Explores the Virtually Human* (Princeton: Princeton University Press, 2008)

[63] Wellman, Boase and Chen argue that virtual communities can provide a sense of belonging and social identity to an individual; see Wellman, B., Boase, J., and Chen, W., 'The Networked Nature of Community: Online and Offline' (2002) 1 (1) *IT & Society,* 151-165

[64] Boellstorff, T., *Coming of age in Second Life: An Anthropologist Explores the Virtually Human* (Princeton: Princeton University Press, 2008) 156

[65] Cerulo, K. A., 'Reframing Social Concepts for a Brave New (Virtual) World' (1997) 67 (1) *Sociological Inquiry*, 48

[66] Williams, M., *Virtually Criminal: Crime, deviance and regulation online* (London: Routledge, 2006); see Basu, R., Mok, D., and Wellman, B., 'Did Distance Matter before the Internet?' (2007) 29 (3) *Social Networks,* 430-461 (analyse the changes in space-time constraints and perceptions of body), see also Shaw, D. B., *Technoculture: The Key Concepts* (New York: Berg, 2008)

[67] See Boellstorff, T., *Coming of age in Second Life: An anthropologist explores the virtually human* (Princeton: Princeton University Press, 2008)

[68] See Boellstorff, T., *Coming of age in Second Life: An anthropologist explores the virtually human* (Princeton: Princeton University Press, 2008)

[69] See Blascovich, J., 'Social influence within immersive virtual environments', in Schroeder, R., (Ed.) *The Social Life of Avatars: Presence and Interaction in Shared Virtual Environments* (London: Springer-Verlag, 2002)127–145

[70] See Rheingold, H., *The Virtual Community: Homesteading on the Electronic Frontier* (2nd Edition) (London: MIT Press, 2000)

[71] Acquisti, A., and Gross, R., 'Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook' (2006) Proceedings of the Sixth Workshop on Privacy Enhancing Technologies

[72] Schaap, F., *The words that took us there: Ethnography in a virtual reality* (Piscataway NJ: Transaction Publishers, 2002)

[73] Castronova, E., 'On the Research Value of Large Games: Natural Experiments in Norrath and Camelot' (2006) 1(2) *Games and Culture*, 163

[74] There is no consistent definition of stalking in law. Within EU, the Member States who have criminal laws covering stalking do not use the term 'stalking' in the definition of the law, opting rather for more generic terms such as 'harassment' and 'persistent pursuit'. See Daphne Project, *Feasibility study to assess the possibilities, opportunities and needs to standardise national legislation on violence against women, violence against children and sexual orientation violence* (Luxembourg: Publications Office of the European Union, 2010). The difficulty in creating an appropriate legal definition of stalking is also due to the distinctive characteristics that set stalking apart from obvious acts of violence or intimidation which normally consist of an isolated illegal act, like rape or physical assault. See Jordan, C. E., Quinn, K., Jordan, B., and Daileader, C. R., 'Stalking: Cultural, clinical and legal considerations' (2000) 38 (3) *Brandeis Journal of Family La*w, 513-579; stalking may involve a series of actions that when looked at individually can seem legal and benign, for example sending gifts or text messaging, is not considered a breach of normative conventions. However, these behaviours are considered criminal if they are part of a pattern of conduct that imparts fear in a victim. See also Keenahan, D., and Barlow, A., 'Stalking: A Paradoxical Crime of the Nineties' (1997) 2 (4) *International Journal of Risk, Security and Crime Prevention,* 291-300

[75] Adam, A., *Gender, Ethics, and Information Technology* (New York: Palgrave Macmillan, 2005) 108

[76] See Picker, R. C., 'Cybersecurity: of Heterogeneity and Autarky', in Grady, M. F., and Parisi, F., (Eds.) *The Law and Economics of Cybersecurity* (CUP, 2005) 115, 117

[77] See Spitzberg, B., and Hoobler, G., 'Cyberstalking and the Technologies of Interpersonal Terrorism' (2002) 4(1) *New Media Society*, 71-92; see also Jewkes, Y., *Media and Crime: Key Approaches to Criminology* (Thousand Oaks: Sage Publications, 2004)

[78] Brenner, S. W., 'Fantasy Crime: The Role of Criminal Law in Virtual Worlds' (2008) 11 (1) *Vanderbilt Journal of Entertainment and Technology Law*, 53, 1-97

[79] See Ashcroft, J., *Stalking and Domestic Violence* (Washington DC: United States Department of Justice, 2001); see also Bocij, P., and McFarlane, L., 'Cyberstalking: The Technology of Hate' (2005) 73 (3) *Police Journal*, 204-221

[80] Wykes, M., 'Constructing Crime: Culture, Stalking, Celebrity and Cyber Crime' (2007) 3 (2) *Media and Culture*, 158-174

[81] For example, stalking in physical space, a vulnerable person, often but not always a woman, can become the target of an individual who insists on a close physical relationship, with escalating, intrusive behaviour calculated to win the victim's affections or, at least, his/her attention. David Letterman, a late-night entertainment show host in the US was such a victim, of a woman who eventually broke into his house. See also Mullen, P., Pathé, M., and Purcell, R., *Stalkers and their Victims* (NY: CUP, 2000)

[82] Also referred to as the transformation test, see for example, Wall, D., *Cybercrimes: The Transformation of Crime in the Information Age* (Cambridge, UK: Polity, 2007)

[83] Wall, D., 'The Internet as a conduit for criminals', in Pattavina, A., (Ed.) *Information Technology and the Criminal Justice System* (Thousand Oaks, CA: Sage, 2005) 77-98; see also Wall, D., *Cybercrimes: The Transformation of Crime in the Information Age* (Cambridge, UK: Polity, 2007)

[84] Wall, D., 'The Internet as a conduit for criminals', in Pattavina, A., (Ed.) *Information Technology and the Criminal Justice System* (Thousand Oaks, CA: Sage, 2005) 79, 77-98

[85] Wall, D., 'The Internet as a conduit for criminals', in Pattavina, A., (Ed.) *Information Technology and the Criminal Justice System* (Thousand Oaks, CA: Sage, 2005) 79, 77-98

[86] Wall, D., *Cybercrimes: The Transformation of Crime in the Information Age*. (Cambridge, UK: Polity, 2007) 47

[87] McGuire, M., *Hypercrime: The New Geometry of Harm* (London: Routledge-Cavendish, 2007) 7

[88] For example Bocij argues that cyberstalking is an entirely new form of criminal behaviour. See Bocij, P., *Cyberstalking: Harassment in the Internet Age and How to Protect Your Family,* (Westport: Praeger

Publishers, 2004); Bocij, P., and McFarlane, L., 'Cyberstalking: The Technology of Hate', (2005) 73 (3) *Police Journal,* 204-221; see also Ashcroft, J., *Stalking and Domestic Violence,* (Washington DC: United States Department of Justice, 2001)

[89] See Basu, S., and Jones, R., 'Regulating Cyberstalking', in Schmalleger, F., and Pittaro, M. (Eds.) *Crimes of the Internet* (Prentice Hall, 2008) 141-165; see also Mullen, P. E., Pathe, M., and Purcell, R., *Stalkers and their Victims* (NY: CUP, 2000) 19

[90] See Reed, C., 'Why Must You Be Mean to Me? Crime and the Online Persona' (2010) 13 (3) *New Criminal Law Review: An International and Interdisciplinary Journal*, 485-514

[91] I have discussed this in the next section.

[92] Reed, C., 'How to Make Bad Law: Lessons from Cyberspace' (2010) 73(6) *Modern Law Review*, 927, 903-932

[93] [2009] EWCACiv 717

[94] McKenna, K. Y. A., Green, A. S., and Gleason, M. E. J., 'Relationship formation on the Internet: What's the big attraction?' (2002) 58 (1) *Journal of Social Issues,* 9-31

[95] Walther found that online interactions are emotionally far more intense than face-to-face interaction. See Walther, J., 'Group and interpersonal effects in international computer-mediated communication' (2007) 23 (3)*Human Communication Research,* 342-369

[96] Meloy J.R., 'The psychology of stalking', in Meloy, J.R., (Ed.) *The Psychology of Stalking: Clinical and Forensic Perspectives* (NY: Academic Press, 1998) 11, 1-23

[97] See Spender, D., *Nattering on the Net* (North Melbourne: Spinifex Press, 1995)

[98] See Williams, M., *Virtually Criminal* (New York: Routledge, 2006)

[99] McGuire, M., *Hypercrime: The New Geometry of Harm* (London: Routledge-Cavendish, 2007) 4

[100] Victims, perpetrators and law enforcement authorities often do not grasp the malicious nature and potential risks associated with 'cyberstalking due to their own and others' misperceptions'. Alexy, Burgess, Baker, and Smoyak describe the dangers associated with such misperceptions and highlighted that victim support service for cyberstalking is virtually non-existent. Alexy, E. M., Burgess, A. W., Baker, T., and Smoyak, S. A., 'Perceptions of Cyberstalking among College Students' (2005) 5 (3) *Brief Treatment and Crisis Intervention*, 280, 279-289

[101] As I have mentioned before by using 'geolocative' social networking application like Foursquare or Google latitude it is possible to know more about an absolute stranger in an hour than one would ever be able to know during face-to-face conversation. During a face-to-face interaction people convey aspects of themselves through a set of signals that which others are able to read and evaluate. See Greenberg, S., 'Threats, Harassment, and Hate On-Line: Recent Developments' (1997) 6 *Boston University Public Interest Law Journal,* 673, 675; see also Ellison, L., 'Cyberstalking: Tackling Harassment on the Internet', in Wall, D., (Ed.)*Crime and the Internet* (Oxon: Routledge, 2001) 141-151

[102] For example, as discussed in '*A Rape in Cyberspace*,' one individual chose to use his account to harass others, resulting in collective aggravation without a real mechanism for stopping the behaviour. See Boyd, D.,*Faceted Id/Entity: Managing Representation in A Digital World* (MIT, 2002)

[103] See Basu, S., and Jones, R., 'Regulating Cyberstalking', in Schmalleger, F. and Pittaro, M., (Eds.) *Crimes of the Internet* (Prentice Hall, 2008) 156

[104] For example, in one Californian case, Gary Dellapenta impersonated the women on-line who did not return his romantic interest. Dellapenta posted web messages indicating that these women wanted to be raped and provided those who responded with the women's names and home addresses. Adam, A., *Gender, Ethics, and Information Technology* (New York: Palgrave Macmillan, 2005); see Valetk, H. A., 'Cyberstalking: Navigating a Maze of Laws', (2002) 228 *NY Law Journal*, 5; see also Lee, R. K., 'Romantic and electronic stalking in a college context' (1998) 4 *William & Mary Journal of Women and the Law*, 373–466

[105] See Basu, S., and Jones, R., 'Regulating Cyberstalking', in Schmalleger, F., and Pittaro, M., (Eds.) *Crimes of the Internet* (Prentice Hall 2008) 141-165; Mullen, P. E., Pathe, M., and Purcell, R., *Stalkers and their Victims* (NY: CUP, 2000) 19

[106] In physical-world commission of an offense involves physical proximity between perpetrator and the victim. Brenner argues that 'this assumption has shaped our approaches to criminal investigation and prosecution'. Brenner, S.W., 'Cybercrime Metrics: Old Wine, New Bottles?' (2004) 9 (13) *Virginia Journal of Law & Technology,* 6,1-52; see also Brenner, S.W., 'Toward A Criminal Law for Cyberspace: Distributed Security' (2004) 10 (1) *Boston University Journal of Science and Technology Law*, 50

[107] Williams, M., *Virtually Criminal: Crime, Deviance and Regulation Online* (London: Routledge, 2006) 19; although the 'cyberstalking victim might not know or see the perpetrator but the psychological impact can still be immense'; see Independent Parliamentary Inquiry into Stalking Law Reform, Main Findings and Recommendations Justice Unions' Parliamentary Group (2012) 15;www.protectionagainststalking.org/InquiryReportFinal.pdf

[108] See Finn, J., 'A survey of online harassment at a University Campus' (2004) 19 (4) *Journal of Interpersonal Violence*, 468-483

[109] Alexy, E. M., Burgess, A. W., Baker, T., and Smoyak, S. A., 'Perceptions of Cyberstalking Among College Students' (2005) 5 (3) *Brief Treatment and Crisis Intervention*, 280-289

[110] Joseph, J., 'Cyberstalking: An International Perspective', in Jewkes, Y., (Ed.) *Dot. Cons: Crime, Deviance and Identity on the Internet* (Collumpton: Willian, 2002) 105-125

[111] Barak, A., 'Sexual harassment on the Internet' (2005) 23 (1) *Social Science Computer Review,* 77-92; see also Finn, J., 'A survey of online harassment at a University Campus' (2004) 19 (4) *Journal of Interpersonal Violence*, 468-483

[112] See http://www.haltabuse.org/resources/stats/Cumulative2000-2009.pdf

[113] See http://www.haltabuse.org/resources/stats/index.shtml

[114] Spitzberg, B. H., and Hoobler, G., 'Cyberstalking and the technologies of interpersonal terrorism' (2004) 4(1) *New Media & Society*, 71–92

[115] See Finn, J. A., 'Survey of Online Harassment at a University Campus' (2004) 19 (4) *Journal of Interpersonal Violence,* 468-483; see also Alexy, E. M., Burgess, A. W., Baker, T., and Smoyak, S. A., 'Perceptions of Cyberstalking among College Students' (2005) 5(3) *Brief Treatment and Crisis Intervention*, 279-289

[116] Maple, C., Short, E., and Brown, A., 'Cyberstalking in the United Kingdom: An Analysis of the ECHO Pilot Survey' (2011) National Centre for Cyberstalking Research

[117] There are currently no methodologically sound international surveys which measure cybercrimes suffered by businesses or home users. See Fafinski, S., Dutton, W.H. and Margetts, H., Mapping and Measuring Cybercrime. (2010) OII Forum Discussion Paper No. 18, Oxford Internet Institute, University of Oxford. See also Wall, D., 'Cybercrime, media and insecurity: the shaping of public perceptions of cybercrime'(2008) 22(1)*International Review of Law, Computers and Technology*, 45

[118] Brenner, S.W., 'Is there such a thing as 'Virtual Crime'?' (2001) 4(1) *California Criminal Law Review, 105*

[119] See Seto, K. W., 'How Should Legislation Deal With Children as the Victims and Perpetrators of Cyberstalking?' (2002) 9 *Cardozo Women's Law Journal*, 67, 73-74

[120] See Brownsword, R., 'Code, control, and choice: Why East is East and West is West' (2005) 25(1) *Legal Studies*, 1; see Brownsword, R., 'Neither East Nor West, Is Mid-West Best?' (2006) 1 (3) *Script-ed*, 15-33; see also Brownsword, R., *Rights, Regulation, and the Technological Revolution* (OUP, 2008) 260

[121] Brownsword, R., 'Neither East Nor West, Is Mid-West Best?' (2006) 1 (3) *Script-ed*, 15-33

[122] To put it differently the regulators are increasingly asked to address the questions of virtual realities that the public encounters.

[123] Wall, D., 'Cybercrime and the Culture of Fear: Social science fiction(s) and the production of knowledge about cybercrime' (2008/11)11(6) *Information, Communication & Society,* 863, 861–884

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

[125] There are legitimate reasons for individuals to interact anonymously on the Internet. The critical challenge is to control the technology without eliminating its legitimate uses.

[126] Reed, C., *Making Laws for Cyberspace* (OUP, 2012) 19

[127] Reed, C., 'How to Make Bad Law: Lessons from Cyberspace' (2010) 73(6) *Modern Law Review*, 927, 903-932

[128] Derogatory or confidential material posted by a cyberstalker is also likely to be covered by defamation and privacy laws (Defamation Act 1996, Article 8 ECHR) which will provide the victim with a means of preventing publication of such material or getting it removed from the internet after publication. A claim in defamation may be made against the cyberstalker (as author of the statement) and the website host (as the publisher of the statement pursuant to the Electronic Commerce (EC Directive) Regulations 2002.

[129] Salter, M., and Bryden, C., 'I can see you: harassment and stalking on the Internet' (2009) 18(2) *Information & Communications Technology Law*, 99-122

[130] The Independent Parliamentary inquiry into stalking Law Reform found that the existing law against harassment is not fit for purpose. The report also claims that victims believe that police do not take them seriously. The inquiry also found that the attitudes of many in the criminal justice system are 'stuck in the dark ages' and view stalking as a 'joke' and believes its victims are 'lucky to get the attention'. See Independent Parliamentary Inquiry into Stalking Law Reform, Main Findings and Recommendations Justice Unions' Parliamentary Group (2012) www.protectionagainststalking.org/InquiryReportFinal.pdf

[131] 2006 UKHL 34

[132] In *Majrowski*, Lord Nicholls set the threshold 'where … the quality of the conduct said to constitute harassment is being examined, courts will have in mind that irritations, annoyances, even a measure of upset, arise at times in everybody's day-to-day dealings with other people. Courts are well able to recognise the boundary between conduct which is unattractive, even unreasonable, and conduct which is oppressive and unacceptable. To cross the boundary from the regrettable to the unacceptable the gravity of the misconduct must be of an order which would sustain criminal liability under section 2' (of the PHA 1977), see *Majrowski v Guys & St Thomas NHS Trust*, 2006 UKHL 34

[133] See Basu, S., and Jones, R., 'Regulating Cyberstalking', in Schmalleger, F., and Pittaro, M., (Eds.) *Crimes of the Internet* (Prentice Hall, 2008) 141-165

[134] University of Modena and Reggio Emilia Modena Group on Stalking, 'Protecting Women from the New Crime of Stalking: a comparison of legislative approaches within the European Union' (University of Modena and Reggio Emilia Modena Group on Stalking, 2007)

[135] Austria, Belgium, Czech Republic, Denmark, Germany, Hungary, Ireland, Italy, Luxembourg, Malta, Netherlands, Sweden, UK

[136] University of Modena and Reggio Emilia Modena Group on Stalking, 'Protecting Women from the New Crime of Stalking: a comparison of legislative approaches within the European Union' (University of Modena and Reggio Emilia Modena Group on Stalking, 2007) 12

[137] It has been suggested to the European Commission to recognise stalking as a criminal offence across all European countries and legislate against it. It is also suggested that EU countries need to co-operate more to gather and share evidence, identify perpetrators and bring them to justice. This would include cross-European enforcement of restraining orders obtained against perpetrators.

[138] To date, all 50 states and the District of Columbia have adopted criminal stalking statutes that target stalking in the physical world. 47 states have enacted cyberstalking specific criminal proscriptions that are subdivisions or specific applications of laws within existing stalking or harassment laws.

[139] http://www.haltabuse.org/resources/stats/index.shtml

[140] Reed, C., 'How to Make Bad Law: Lessons from Cyberspace' (2010) 73(6) *Modern Law Review*, 927, 903-932

[141] Reed, C., 'How to Make Bad Law: Lessons from Cyberspace' (2010) 73(6) *Modern Law Review*, 927, 903-932

[142] See Basu, S., and Jones, R., 'Regulating Cyberstalking', in Schmalleger, F., and Pittaro, M., (Eds.) *Crimes of the Internet* (Prentice Hall, 2008) 141-165. Similarly Ellison also argues that 'the positive value of anonymous communication more than offsets the dangers and restrictions on anonymity on-line would be both premature and harmful to individual users and to the Internet community at large'. Ellison, L., 'Cyberstalking: Tackling Harassment on the Internet', in Wall, D., (Ed.) *Crime and the Internet* (Oxon: Routledge, 2001) 147, 141-151

[143] Andersen, B., 'Shackling the digital economy means less for everyone: the impact on the music industry', (2010) 28 (4) *Prometheus*, 375, 375-383

[144] Bowery, K., 'The New, the Bad, the Hot, the Fad - popular music, technology and the culture of freedom', in Macmillan, F., (Ed.) *New Directions in Copyright Law: Volume 2* (Cheltenham: Edward Elgar, 2005) 262-271

[145] Salter, M., and Bryden, C., 'I can see you: harassment and stalking on the Internet' (2009) 18(2) *Information & Communications Technology Law*,99-122

[146] Salter, M., and Bryden, C., 'I can see you: harassment and stalking on the Internet' (2009) 18(2) *Information & Communications Technology Law*,116, 99-122

[147] The dominant model for the exercise of legal authority is deterrence which is based on the rational choice view of human behaviour. See Paternoster, R., 'How Much Do We Really Know About Criminal Deterrence?' (2006) 100 *Journal of Criminal Law and Criminology*, 765-824, see also Reed, C., *Making Laws for Cyberspace* (OUP, 2012) 10

[148] There is a multitude of legal definitions of stalking, meaning, behaviour that would constitute stalking in one jurisdiction would not necessarily meet the criteria required in another and stalking as such is not criminalised in many countries. See McEwan, T.E., Mullen, P.E., and MacKenzie, R., 'Anti-Stalking Legislation in Practice: Are we meeting community needs?' (2007) 14 (2) *Psychiatry, Psychology and Law*, 207-217

[149] Reed, C., 'How to Make Bad Law: Lessons from Cyberspace' (2010) 73(6) *Modern Law Review*, 927, 903-932

[150] For a discussion on factors that make it difficult for law enforcement authorities to prosecute perpetrators of cybercrime; see Brenner, S.W., and Schwerha, J IV., 'Transnational Evidence-Gathering and Local Prosecution of International Cybercrime' (2002) 20 (3) *John Marshall Journal of Computer & Information Law*, 347-395; see also Brenner, S.W., and Koops, B., 'Approaches to Cybercrime Jurisdiction' (2004) 4 (3)*Journal of High Technology Law,* 3-44

[151] See Hart, H.L.A., 'A More Recent Positivist Conception of Law', in *The Concept of Law* (Oxford: Oxford University Press, 1961)

[152] There is a need to review laws around the penumbra that deals particularly with child grooming in order to make sure that such laws cover the areas that should be legislated.

[153] See Murray, A.D., *The Regulation of Cyberspace* (Abingdon: Routledge-Cavendish, 2007)

[154] See Biegel, S., *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace* (Cambridge, MA: MIT Press, 2003)

[155] See Murray, A.D., *The Regulation of Cyberspace* (Abingdon: Routledge-Cavendish, 2007)

[156] Murray, A.D., *The Regulation of Cyberspace* (Abingdon: Routledge-Cavendish, 2007) 243

[157] Murray, A.D., *The Regulation of Cyberspace* (Abingdon: Routledge-Cavendish, 2007) Ch-8

[158] Wall, D., and Williams, M., 'Policing diversity in the digital age: Maintaining order in virtual communities' (2007) 7 (4) *Criminology and Criminal Justice,* 391-415

[159] Biegel, S., *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace* (Cambridge: Mass: MIT Press, 2003)

[160] Biegel believes that placing problematic behaviour into one of these four categories makes it easier to identify common characteristics the 'cyberproblems' share. The first category is 'dangerous conduct', anything that 'may impact physical or national safety'. The second is 'fraudulent conduct', defined as activity that 'may impact economic safety'. The third category encompasses other 'unlawful anarchic conduct',

including illegal activity that does not clearly fit into the first two categories. Finally, the 'inappropriate conduct' category catches what remains: lawful behaviour that is nonetheless 'troubling' to some. Cyberstalking would fall under the first category. See Biegel, S., *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace* (Cambridge: Mass: MIT Press, 2003) 55-85

[161] First, identification of the category of the problematic conduct by placing the behaviour into one of four broad categories; second, potential for consensus among the various stakeholders regarding both the nature and the extent of the problem and the prospects for any sort of regulatory solution; third, uniqueness of the problem; whether the problem is uniquely cyber, or if an existing regulatory scheme could address it; fourth; evaluation of the potential effectiveness of the three regulatory models as identified by him and finally, at step five the regulator must consider the impact of each regulatory model in combination with the others and predict whether any regulation could adequately address the potential problem at this time. See Biegel, S., *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace* (Cambridge: Mass: MIT Press, 2003) 224-225

[162] Biegel, S., *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace* (Cambridge, Mass: MIT Press, 2003) 53

[163] Biegel derives from the framework his 'list of relevant principles that can help guide the regulatory process across the board'. See Biegel, S., *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace* (Cambridge: Mass: MIT Press, 2003) 359

[164] See Biegel, S., *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace* (Cambridge: Mass: MIT Press, 2003) 359,360

[165] Brenner, S.W., 'Is There Such a Thing as 'Virtual Crime'?' (2001) 4(1) *California Criminal Law Review,* 105

[166] Wall, D., 'Digital Realism and the Governance of Spam as Cybercrime' (2004) 10 (4) *European Journal on Criminal Policy and Research*, 309-355

[167] See Basu, S., and Jones, R., 'Regulating Cyberstalking', in Schmalleger, F. and Pittaro, M., (Eds.) *Crimes of the Internet* (Prentice Hall, 2008) 141-165

[168] Brownsword, R., Neither East Nor West, Is Mid-West Best? (2006) 1(3) *Script-ed*, 15-33

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

[170] *LICRA v Yahoo* (2000)

[171] Preece argues that virtual communities would benefit from clear policies and rules. Preece, J., 'Etiquette Online: From Nice to Necessary' (2004) 47(4) *Communications of the Association of Computing Machinery,* 56–61

[172] 'In many contexts, law is not central to the maintenance of social order'. See Ellickson, R.C., *Order without Law: How Neighbours Settle Disputes* (Cambridge: Mass-Harvard University Press, 1991) 280; see also Huang, P. H., and Wu, H., 'More Order without More Law: A Theory of Social Norms and Organizational Cultures' (1994) 10 (2) *Journal of Law Economics & Organisation*, 390-406

[173] See Stoup, P., 'The Development and Failure of Social Norms in Second Life' (2008) 58 (2) *Duke Law Journal*, 311-344; Kerr also argues that a 'strong regime of criminal enforcement would threaten one of the foundational strengths of virtual world, the ability of each virtual world to define its own terms'. See Kerr, O. S., 'Criminal Law in Virtual Worlds' (2008) *University of Chicago Legal Forum*, 427, 415-429; see also Lastowka, G. F., and Hunter, D., 'The Laws of the Virtual Worlds' (2004) 92 (1) *California Law Review*, 7, 3-74

[174] Reed, C., 'How to Make Bad Law: Lessons from Cyberspace' (2010) 73(6) *Modern Law Review*, 927, 903-932

[175] Lessig, L., *Code and other Laws of Cyberspace* (New York: Basic Books, 1999)

[176] Durkheim, E., *The Division of Labor in Society* (George Simpson trans., The Free Press 1964) (1893), 79-80

[177] Virtual communities can be governed by its own set of rules based on the principle 'any free society must be governed by its own rules.' See Mayer-Schonberger, V., 'The Shape of Governance: Analysing the World of Internet Regulation' (2003) 43 (3) *Virginia Journal of International Law* , 605

[178] As discussed before the philosophical basis of 'protocols' is similar to 'communitarianism', particularly 'responsive communitarianism'. See Bell, D., 'Communitarianism', in Zalta, E. N., (Ed.) *The Stanford Encyclopaedia of Philosophy* (Spring, 2005).See also Etzioni, A., et al., 'The *Responsive Communitarian* Platform: Rights and Responsibilities', in Schumaker, P., (Ed.) *The Political Theory Reader* (MA: Wiley-Blackwell, 2010) 231

[179] For example norms created and enforced by the residents and the operators of Second Life. It is a list of community standards, the 'Big Six' and a general standard guiding- residents' behaviour. See Second Life Community Standards, including 'intolerance', 'harassment', 'assault', 'disclosure', 'Adult Regions, Groups and Listings' and 'Disturbing the Peace'. available at: http://secondlife.com/corporate/cs.php

[180] The psychological predispositions lead individuals in communities to more willingly work with others to address the needs of their community. See Tyler, T.R., *Why People Cooperate* (Princeton: Princeton University Press, 2011)

[181] The 'collective conscience' is defined as the totality of beliefs and sentiments common to members of the same society (in this case it is the virtual community) that form a determinate system which has its own life. Without this consensus there is nothing to distinguish norms imposed by a community from the rough justice of the vigilante. Durkheim, E., *The Division of Labor in Society* (George Simpson trans., The Free Press 1964) (1893), 79-80

[182] The essence of this approach is to ensure that the individuals in the virtual community engage with the protocols because they consider it as their social and moral responsibility towards the virtual community, similar to recycling or not parking in handicap spaces. See Bell, D., 'Communitarianism', in Zalta, E. N., (Ed.) *The Stanford Encyclopaedia of Philosophy* (Spring, 2005). See Etzioni, A., et al., 'The *Responsive Communitarian*Platform: Rights and Responsibilities', in Schumaker, P. (Ed.) *The Political Theory Reader* (MA: Wiley-Blackwell, 2010) 231; similarly eBay, for example, makes use of the community norms and practices to influence the way in which participants behave on the auction site; see also Suzor, N., 'Order Supported by Law: The Enforcement of Rules in Online Communities' (2012) 63 *Mercer Law Review*, 523-595

[183] Ellickson's exploratory research referring to dispute solution for a dispute about strayed cattle in Shasta County, California shows that social norms can overrule the law in force. To establish these norms within a group of people, three conditions must be satisfied: 1. All group members have the ability and power to administer punishments or sanctions; 2. each member must have the opportunity to exercise the power; 3. each member has adequate historical and current information about every member's social interactions. The extent to which these conditions are satisfied will determine how effective the monitoring and sanctioning powers are, resulting in the successful establishment of social norms within the community. See Ellickson, R.C., *Order without Law: How Neighbours Settle Disputes* (Cambridge: Mass-Harvard University Press, 1991) 179; this form of governance also reflects Foucault's understanding of 'governmentality', see Foucault, M., 'The Subject and Power', in Dreyfus, H. L., and Rabinow, P., (Eds.) *Michel Foucault: Beyond Structuralism and Hermeneutics : with an afterthought by Michel Foucault* (Brighton: Harvester Press, 1982)

[184] It is not surprising that on-line dating has led to cyberstalking but that does not mean we should legislate for it.

[185] Berman called upon courts to take into account of the fact that legal norms are not produced exclusively by governments. Berman, P. S., 'Globalization of Jurisdiction' (2002) 151 (2) *University of Pennsylvania Law Review*, 390; see also Berman, P. S., 'Towards a Cosmopolitan Vision of Conflict of Laws: Redefining Governmental Interests in a Global Era' (2005) 153 (6) *University of Pennsylvania Law Review*, 1819

[186] Fairfield has also emphasised the role of consent for establishing legitimacy of norms of a virtual community, see Fairfield, J., 'The Magic Circle' (2009) 11 (4) *Vanderbilt Journal of Entertainment and Technology Law*, 823–840

[187] See Ellison, L., 'Cyberstalking: Tackling Harassment on the Internet', in Wall, D., (Ed.) *Crime and the Internet* (Oxon: Routledge, 2001) 141-151. As mentioned before due to misperceptions, victims and law enforcement authorities often do not understand the risks associated with cyberstalking. See Alexy, E. M.,

Burgess, A. W., Baker, T., and Smoyak, S. A., 'Perceptions of cyberstalking among college students', 5 (3) *Brief Treatment and Crisis Intervention,* 280*,* 279-289

[188] Wall, D., and Williams, M., 'Policing diversity in the digital age: Maintaining order in virtual communities' (2007) 7 (4) *Criminology and Criminal Justice*, 402, 391-415. See also Taylor, T. L., *Play between Worlds: Exploring Online Game Culture* (Cambridge: MIT Press, 2006)

[189] From a social capital perspective, psychological (positive values, attitudes) and sociological factors that predispose communities would also ensure the effective cooperation. See Tyler, T.R., *Why People Cooperate*(Princeton: Princeton University Press, 2011)

[190] The 'positive consensus' would ensure that the minorities are not unduly disadvantaged by the 'collective sentiments' of the majority. Hence each person who has an interest in the maintenance of the protocols and the application of sanctions to those who violate it would have an interest in spreading of the information that can lead to a consensus on acceptable sanctions and avoid unintended consequences. Etzioni argues that the 'majoritarian' dangers of communities can and should be counter-balanced by enforcement of the 'overarching values' we all share. Etzioni, A., *The Spirit of Community: Rights, Responsibilities and the Communitarian Agenda* (Fontana Press,1995)

[191] For example in 'Second Life' deviant behaviour of an inhabitant get publicised in weblogs and websites. Wall also claims that the bond a user shares with other users and the virtual community is 'as significant as offline ties', see Wall, D., and Williams, M., 'Policing diversity in the digital age: Maintaining order in virtual communities' (2007) 7 (4) *Criminology and Criminal Justice*, 404, 391-415; see also Stoup, P., 'The Development and Failure of Social Norms in Second Life' (2008) 58 (2) *Duke Law Journal*, 320, 311-344

[192] For a discussion on community enforcement of norms; see Grimmelmann, J., 'Virtual World Feudalism' (2009) 118 *Yale Law Journal Pocket Part,* 126; see also Balkin, J., 'Virtual Liberty: Freedom to Design and Freedom to Play in Virtual Worlds' (2004) 90 (8) *Virginia Law Review*, 2043, 2044, 2062

[193] The conceptual similarity to the 'control theory' should be noted here which assumes the existence of a common value system within the society or group. There are four crucial bonds which bind us together: attachment, commitment, involvement and belief. Involvement refers to behavioural investments in conventional lines of action that could preclude involvement in deviant behaviour. Belief refers to how strong is a person's sense that they should obey the rules of society. Hirschi, T., *Causes of Delinquency* (Berkeley: University of California Press, 1969). Further, sociologists, such as, Sykes and Matza have argued that people become deviant only when they find it is possible to justify illegal or deviant behaviour. It is my argument that the bond between the virtual community and the individual will always ensure that there is less opportunity to justify such action; see Sykes, G. M., and Matza, D., 'Techniques of Neutralization: A Theory of Delinquency' (1957) 22 (6) *American Sociological Review*, 664-670

[194] Ellickson found similar behavioural pattern among the ranchers in the Shasta County, see Ellickson, R., *Order without Law: How Neighbors Settle Disputes* (Cambridge: Harvard University Press, 1991) 57; this is also consistent with social psychological research showing that people want to feel valued members of social groups, see Tyler, T.R., and Blader, S., *Cooperation in groups: Procedural justice, social identity, and behavioral engagement* (Philadelphia: Psychology Press, 2000); Tyler, T.R., Degoey, P., and Smith, H., 'Understanding why the justice of group procedures matters: A test of the psychological dynamics of the group-value model' (1996) 70 *Journal of Personality and Social Psychology*, 913-930

[195] Schrock, A. and Boyd, D., 'Problematic Youth Interaction Online: Solicitation, Harassment, and Cyberbullying', (2011) in Wright, K.B., and Webb, L. M., (Eds.) *Computer-Mediated Communication in Personal Relationships* (New York: Peter Lang)

[196] See Schrock, A. and Boyd, D., 'Problematic Youth Interaction Online: Solicitation, Harassment, and Cyberbullying', (2011) in Wright, K.B., and Webb, L. M., (Eds.) *Computer-Mediated Communication in Personal Relationships* (New York: Peter Lang)

[197] See Reid, E., 'Hierarchy & Power: Social Control in Cyberspace', in Kollock, P., and Smith, A., (Eds.) *Communities in Cyberspace* (London: Routledge, 1999) 107–133

[198] Wall, D., and Williams, M., 'Policing diversity in the digital age: Maintaining order in virtual communities' (2007) 7 (4) *Criminology and Criminal Justice*, 404, 391-415

[199] Biegel, S., *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace* (Cambridge: Mass, MIT Press, 2003) 21

[200] For example, such a situation will arise if virtual communities are formed according to interests in extreme or negatively viewed behaviours or with the intent to share mutual deviant proclivities, e.g. paedophiles or self-injurers. There is evidence to suggest that virtual communities provide a kind of safety and freedom to paedophiles or self-injurers that runs counter to their deviant loner status in the real world. Jenkins, P., *Beyond tolerance: Child pornography on the Internet* (New York: New York University Press,2001); see also Adler, P. A. and Adler, P., 'The cyber worlds of self-injurers: Deviant communities, relationships, and selves' (2008) 31(1)*Symbolic Interaction*, 33–56

[201] It is important that activities within the virtual communities be required to conform to conventional legal requirements within a host jurisdiction. However, content analysis of hate groups suggests that very few of them openly espouse hatred or advocate for violence even if they are violent groups. This is also further complicated by lack of international harmonisation of cybercrime laws. Douglas, K. M., McGarty, C., Bliuc, A.M., and Lala, G., 'Understanding Cyberhate: Social competition and social creativity in online white supremacist groups' (2005) 23 (1) *Social Science Computer Review,* 68–76; see Gerstenfeld, P. B., Grant, D. R., and Chiang, C.P., 'Hate online: A content analysis of extremist websites' (2003) 3(1) *Analyses of Social Issues and Public Policy,* 29–44; see also Smith, R. Grabosky, P., and Urbas, G., *Cybercriminals on trial* (Cambridge: CUP, 2004); further, for an in-depth analysis of the interplay between racism and the cyberspace, see Kang, J., 'Cyber-Race' (2000) 113 (5) *Harvard Law Review,* 1130-1209

[202] Durkheim defined deviant behaviour as that which 'fails to conform to the rules or norms of the group in question'. This means that a group's terms would determine whether a particular act is normal or deviant. See Durkheim, E., *Moral Education* (Free Press, 1960); for example, 'EVE Online' encourages fraud and theft and users do not see their choices as morally wrong. However, 'mandated lawlessness is still lawlessness'. Wilson and Herrnstein argue that deviant behaviour, like all other human behaviour, is a product of a rational choice by the individual. Wilson, J. Q., and Herrnstein, R. J., *Crime and Human Nature* (Simon and Schuster: New York, 1985); see also Risch, M., 'Virtual Rule of Law' (2009) 112 (1) *West Virginia Law Review*, 10, 42, 1-50

[203] Bonnici, J.P. M., and Cannataci, J.A., 'Access to information: controlling access to information as a means of internet governance' (2003) 17 (1) *International Review of Law Computers and Technology*, 51

[204] For example, Linden Lab threatened to ban anyone who takes part in paedophilic role-playing in *Second Life.* This ban was imposed to avoid any liability when the US criminalised virtual child pornography (*Child Pornography Prevention Act* 1996). See Simpson, B., 'What happens online stays online? Virtual punishment in the real world' (2011) 20 (1) *Information & Communications Technology Law*, 7, 3-17

[205] Suzor, N., 'Order Supported by Law: The Enforcement of Rules in Online Communities' (2012) 63 (2) *Mercer Law Review*, 524, 523-595; Brenner similarly argues that delinquent behaviour which causes harm that and which is 'limited to the virtual experiential context' should be dealt with within the virtual community, but those deviant behaviours which have far more outreaching effect and cause substantial harm in the victim's life in the physical world must be appropriately dealt with by the criminal laws, see Brenner, S. W., 'Fantasy Crime: The Role of Criminal Law in Virtual Worlds' (2008) 11 (1) *Vanderbilt Journal of Entertainment and Technology Law*, 60, 1-97; see Kerr, O. S., 'Criminal Law in Virtual Worlds' (2008) *University of Chicago Legal Forum*, 425, 415-429 (criminal law should be potentially available to remedy wrongs that cannot be redressed within the virtual community). Importantly, it can also be argued that the prospect of external intervention should be kept as the last resort as it may cause instability within the virtual community by calling into question the legitimacy of protocols. See also Post, D. G., 'Governing *Cyberspace: Law*' (2008) 24 (4) *Santa Clara Computer & High Technology Law Journal*, 883-913 (argues that legitimate internal governance by virtual communities may not emerge if there is always a threat of external interference).

[206] Ellickson, R. , *Order Without Law: How Neighbors Settle Disputes* (Cambridge: Harvard University Press, 1991)

[207] Another, slightly more complex solution would be to ban IP addresses so as to prevent a banned or suspended user from access to the virtual community through their network connection. Again, the user could get around this by either logging on from a different internet connection or by using one of the freely available online tools to change the IP address. However, it can also be argued that the longer one participates in a community, the more irreversible commitments (social or economic) he/she may make, and

the harder it becomes to leave. See Burk, D. L., 'Virtual Exit in the Global Information Economy' (1999) 73 (4) *Chicago Kent Law Review*, 943, 943-996

[208] *eBay's* peer review and reputation analysis system allows users to leave feedback about another user. This system allows users to build up a reputation profile over time, based on comments and ratings given by other users. It provides a means of control over the anonymous users. This system can be incorporated within virtual communities, with the reputation system containing information about participants' past and present behaviour. See 'How Feedback Works', http://pages.ebay.com/help/feedback/howitworks.html

[209] *eBay's* peer review and reputation analysis system allows users to leave feedback about another user. This system allows users to build up a reputation profile over time, based on comments and ratings given by other users. It provides a means of control over the anonymous users. This system can be incorporated within virtual communities, with the reputation system containing information about participants' past and present behaviour. See 'How Feedback Works', http://pages.ebay.com/help/feedback/howitworks.html

[210] One of the main benefits of this system is that it should prevent users from creating new accounts, since it would be harder for someone with no reviews to socialise. See 'How Feedback works,' available at http://pages.ebay.com/help/feedback/howitworks.html

[211] Goldsmith, J., and Wu, T., *Who Controls The Internet? Illusions of a Borderless World* (OUP, 2006) 129; Stoup argued for an optimal mix between code-created rules and real-world regulations at the lowest cost. See Stoup, P., 'The Development and Failure of Social Norms in Second Life' (2008) 58 (2) *Duke Law Journal,* 313, 311-344

[212] Dibbell, J., 'Owned! Intellectual property in the age of eBayers, gold farmers, and other enemies of the virtual state', in Balkin, J. M., and Noveck, B. S., (Eds.) *The State of Play: Law, Games, and Virtual Worlds (*New York and London: New York University Press, 2006) 144, 137-145

[213] 'The rule of law requires some form of due process: that is, a process reasonably designed to ascertain the truth . . . as to whether a violation has taken place and under what circumstances'; see Rawls, J., *A theory of justice* (Cambridge: Harvard, 1971) 239

[214] Grimmelmann, J., 'Virtual Worlds as Comparative Law' (2004) 49 *New York Law School Law Review*, 180, 147-181

[215] See Castronova, E., *Synthetic Worlds*: *The business and culture of online games* (Chicago: The University of Chicago Press, 2005) 127

[216] Edelstein, J. I., 'Anonymity and International Law Enforcement in Cyberspace'(1996) 7 *Fordham Intellectual Property, Media & Entertainment Law Journal*, 231, 284-86

[217] Lindenberg, S., 'Grounding Groups in Theory: Functional, Cognitive and Structural Interdependencies', in Lawler, E. J., (Ed.) *Advances in Group Processes* (Greenwich, CT: JAI Press, 1997) 281–331

[218] Protocols can be unduly moralistic and majoritarian in attempting to articulate the vision of ethical conduct.

[219] It can be argued that the enforcement of community norms, even if enforcement is effective some of the time, may not always provide sufficient widespread stability. Williams, M., *Virtually Criminal: Crime, Deviance and Regulation Online* (London: Routledge, 2006) 138; Goldsmith, J., and Wu, T., *Who Controls The Internet? Illusions of a Borderless World* (OUP, 2006) 135; see Arias, A 'Life, Liberty, and the Pursuit of Swords and Armor: Regulating the Theft of Virtual Goods' (2008) 57 (5) *Emory Law Journal*, 1340, 1341, 1301-1346; Stoup argued that there are too many users to regulate; see Stoup, P., 'The Development and Failure of Social Norms in Second Life' (2008) 58 (2) *Duke Law Journal*, 328, 311-344; but if norms are accepted, then norms can have a real-world effect. See Fairfield, J., 'The Magic Circle' (2009) 11(4) *Vanderbilt Journal of Entertainment and Technology Law*, 831,832, 823-840

[220] For example, Second Life's norm-based sanctions against individuals who committed undesirable behaviours proved to be limitedly effective as participants only have limited capabilities to administer sanctions. See Stoup, P., 'The Development and Failure of Social Norms in Second Life' (2008) 58 (2) *Duke Law Journal,* 311-344; see also Carr, P., and Pond, G., *The Unofficial Tourists' Guide to Second Life* (Oxford: Pan Macmillan Ltd, 2007)

[221] Consent is key to determine allowable conduct in virtual worlds, Fairfield, J., 'The Magic Circle' (2009) 11 (4) *Vanderbilt Journal of Entertainment and Technology Law*, 832, 823-840; see Rothchild, J., 'Protecting

the Digital Consumer: The Limits of Cyberspace Utopianism' (1999) 74 (3) *Indiana Law Journal*, 967,968,893-998; but Grimmelmann highlighted the importance of forming and enforcing social norms despite their weaknesses; see Grimmelmann, J., 'Virtual Worlds as Comparative Law' (2004) 49 *New York Law School Law Review*, 170,147-181

Bibliography

Adam, A., *Gender, Ethics, and Information Technology* (New York: Palgrave Macmillan, 2005)

Adler, P. A., and Adler, P., 'The cyber worlds of self-injurers: Deviant communities, relationships, and selves' (2008) 31(1) *Symbolic Interaction,* 33–56

Alexander, G.S., 'Dilemmas of Group Autonomy: Residential Associations and Community' (1989) 75 (1) *Cornell Law Review*, 17–33

Alexy, E. M., Burgess, A. W., Baker, T., and Smoyak, S. A., 'Perceptions of Cyberstalking among College Students' (2005) 5 (3) *Brief Treatment and Crisis Intervention*, 279-289

Andersen, B., 'Shackling the digital economy means less for everyone: the impact on the music industry' (2010) 28 (4) *Prometheus*, 375, 375-383

Arias, A., 'Life, Liberty, and the Pursuit of Swords and Armor: Regulating the Theft of Virtual Goods' (2008) 57 (5) *Emory Law Journal*, 1301-1346

Ashcroft, J., *Stalking and Domestic Violence* (Washington DC: United States Department of Justice, 2001)

Basu, S., and Jones, R., 'Regulating Cyberstalking', in Schmalleger, F. and Pittaro, M., (Eds.) *Crimes of the Internet* (Prentice Hall, 2008) 141-165

Basu, R., Mok, D., and Wellman, B., 'Did Distance Matter before the Internet?' (2007) 29 (3) *Social Networks,* 430-461

Balkin, J., 'Virtual Liberty: Freedom to Design and Freedom to Play in Virtual Worlds' (2004) 90 (8) *Virginia Law Review*, 2043-2098

Barfield, W., 'Intellectual Property Rights in Virtual Environments: considering the rights of owners, programmers and virtual avatars' (2006) 39 *Akron Law Review*, 649-700

Barak, A., 'Sexual harassment on the Internet' (2005) 23 (1) *Social Science Computer Review,* 77-92

Beck, U., and Beck-Gernsheim, E., *Individualization* (London: Sage, 2002)

Bell, D., 'Communitarianism', in Zalta, E. N., (Ed.) *The Stanford Encyclopaedia of Philosophy* (Spring, 2005)

Berman, P. S., 'Globalization of Jurisdiction' (2002) 151(2) *University of Pennsylvania Law Review*, 391-529

Berman, P. S., 'Towards a Cosmopolitan Vision of Conflict of Laws: Redefining Governmental Interests in a Global Era' (2005) 153 (6) *University of Pennsylvania Law Review,* 1819-1882

Biegel, S., *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace* (Cambridge: Mass: MIT Press, 2003)

Blascovich, J., 'Social influence within immersive virtual environments', in Schroeder, R., (Ed.) *The Social Life of Avatars: Presence and Interaction in Shared Virtual Environments* (London: Springer-Verlag, 2002) 127–145

Bocij, P., and McFarlane, L., 'Cyberstalking: The Technology of Hate' (2005) 73 (3) *Police Journal*, 204-221

Bocij, P., *Cyberstalking: Harassment in the Internet Age and How to Protect Your Family* (Westport: Praeger Publishers, 2004)

Boal, I.A., 'A flow of monsters: Luddism and virtual technologies', in Brook, J., and Boal, I.A., (Eds.) *Resisting the Virtual Life: the Culture and Politics of Information*, (San Francisco: City Lights, 1995) 3-15

Bowery, K., 'The New, the Bad, the Hot, the Fad - popular music, technology and the culture of freedom', in Macmillan, F., (Ed.) *New Directions in Copyright Law*: *Volume 2* (Cheltenham: Edward Elgar, 2005) 262-271

Boellstorff, T., *Coming of age in Second Life: An Anthropologist Explores the Virtually Human* (Princeton: Princeton University Press, 2008)

Boyd, D., *Faceted Id/Entity: Managing Representation in a Digital World* (MIT, 2002)

Bonnici, J.P.M., and Cannataci, J.A., 'Access to information: controlling access to information as a means of internet governance' (2003) 17 (1) *International Review of Law Computers and Technology*, 51-62

Brenner, S. W., 'Fantasy Crime: The Role of Criminal Law in Virtual Worlds' (2008) 11 (1) *Vanderbilt Journal of Entertainment and Technology Law* , 1-97

Brenner, S. W*.,* 'Distributed Security: Moving Away from Reactive Law Enforcement' (2005*)* 9 *International Journal of Communications Law & Policy,* 1-43

Brenner, S.W., 'Is There Such a Thing as 'Virtual Crime'?' (2001) 4(1) *California Criminal Law Review*, 105-111

Brenner, S.W., 'Toward A Criminal Law for Cyberspace: Distributed Security' (2004) 10 (1) *Boston University Journal of Science and Technology Law*, 50

Brenner, S.W., 'Cybercrime Metrics: Old Wine, New Bottles?' (2004) 9 (13) *Virginia Journal of Law & Technology,* 1-52

Brenner, S.W., and Koops, B., 'Approaches to Cybercrime Jurisdiction' (2004) 4 (3) *Journal of High Technology Law,* 3-44

Brenner, S.W., and Schwerha, J IV., 'Transnational Evidence-Gathering and Local Prosecution of International Cybercrime' (2002) 20 (3) *John Marshall Journal of Computer & Information Law*, 347-395

Brownsword, R., *Rights, Regulation, and the Technological Revolution* (OUP, 2008)

Brownsword, R., 'Neither East Nor West, Is Mid-West Best?' (2006) 1(3) *Script-ed*, 15-33

Brownsword, R., 'Code, control, and choice: Why East is East and West is West' (2005) 25(1) *Legal Studies*, 1

Buss, A., and Strauss, N., *Online Communities Handbook: Building your Business and Brand on the Web* (Berkeley: New Riders, 2009)

Burk, D. L., 'Virtual Exit in the Global Information Economy' (1999) 73 (4) *Chicago Kent Law Review*, 943-996

Cairncross, F., *The Death of Distance: How the Communications Revolution will Change Our Lives* (Harvard Business Press, 2001)

Calhoun, C., 'Indirect Relationships and Imagined Communities: Large-Scale Social Integration and the Transformation of Everyday Life', in Bourdieu, P., and Coleman, J.S., (Eds.) *Social Theory for a Changing Society*(San Francisco-Oxford: Boulder, 1991) 95-121

Carr, P., and Pond, G., *The Unofficial Tourists' Guide to Second Life* (Oxford: Pan Macmillan Ltd, 2007)

Castronova, E., *Synthetic Worlds*: *The business and culture of online games* (Chicago: The University of Chicago Press, 2005)

Castronova, E., 'On the Research Value of Large Games: Natural Experiments in Norrath and Camelot' (2006) 1(2) *Games and Culture*, 163-186

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

Chik, W., 'Harassment through the Digital Medium A Cross-Jurisdictional Comparative Analysis on the Law on Cyberstalking' (2008) 3(1) *Journal of International Commercial Law and Technology*, 13-44

Coates, J., Suzor, N., and Fitzgerald, A., *Legal aspects of web 2.0 activities: Management of legal risk associated with the use of YouTube, MySpace and Second Life (*Brisbane: ARC Centre of Excellence for Creative Industries and Innovation and Queensland University of Technology, 2007)

Cooke, M., and Buckley, N., 'Web 2.0, Social Networks and the Future of Market Re-search' (2008) 50 (2) *International Journal of Market Research* , 267–292

Daphne Project, 'Feasibility study to assess the possibilities, opportunities and needs to standardise national legislation on violence against women, violence against children and sexual orientation violence' (Luxembourg: Publications Office of the European Union, 2010)

Demetriou, C., and Silke, A., 'A Criminological Internet 'Sting': Experimental Evidence of Illegal and Deviant Visits to a Website Trap' (2003) 43(1) *The British Journal of Criminology*, 213-222

Deibert, R. J., and Rohozinski, R., 'Risking Security: Policies and Paradoxes of Cyberspace Security' (2010) 4 (1) *International Political Sociology*, 15–32

Dibbell, J., 'Owned! Intellectual property in the age of eBayers, gold farmers, and other enemies of the virtual state', in Balkin, J. M., and Noveck, B. S., (Eds.) *The State of Play: Law, Games, and Virtual Worlds* (New York and London: New York University Press, 2006) 137-145

Douglas, K. M., McGarty, C., Bliuc, A.M., and Lala, G., 'Understanding Cyberhate: Social competition and social creativity in online white supremacist groups' (2005) 23 (1) *Social Science Computer Review,* 68–76

Durkheim, E., *The Division of Labor in Society* (George Simpson trans., The Free Press 1964) (1893), 79-80

Durkheim, E., *Moral Education* (Free Press, 1960)

Edelstein, J. I., 'Anonymity and International Law Enforcement in Cyberspace' (1996) 7 *Fordham Intellectual Property , Media & Entertainment Law Journal*, 231, 284-86

Ellison, L., 'Cyberstalking: Tackling Harassment on the Internet', in Wall, D., (Ed.) *Crime and the Internet* (Oxon: Routledge, 2001) 141-151

Ellickson, R.C., *Order without Law: How Neighbours Settle Disputes* (Cambridge: Mass-Harvard University Press, 1991)

Etzioni, A., (Ed.) *The Essential Communitarian Reader* (Maryland: Rowman & Littlefield, 1998)

Etzioni, A., *et al*., 'The *Responsive Communitarian* Platform: Rights and Responsibilities', in Schumaker, P., (Ed.) *The Political Theory Reader* (MA: Wiley-Blackwell, 2010) 231

Etzioni, A., *The Spirit of Community: Rights, Responsibilities and the Communitarian Agenda* (Fontana Press,1995)

Fafinski, S., Dutton, W.H., and Margetts, H., 'Mapping and Measuring Cybercrime' (2010) OII Forum Discussion, Paper No. 18 (Oxford: Oxford Internet Institute, University of Oxford)

Fairfield, J., 'The Magic Circle' (2009) 11 (4) *Vanderbilt Journal of Entertainment and Technology Law*, 823–840

Fernback, J., 'The Individual within the Collective: Virtual Ideology and Realisation of Collective Principles', in Jones, S., (Ed.) *Virtual Culture* (London: Sage Publications, 1997) 36–54

Finn, J., 'A survey of online harassment at a University Campus' (2004) 19(4) *Journal of Interpersonal Violence*, 468-483

Filosa, G., *Online profiles attracting sexual predators, feds warn; Teen sites being used as victim directories* (The Times- Picayune, 2007)

Foucault, M., 'The Subject and Power', in Dreyfus, H. L., and Rabinow, P., (Eds.) *Michel Foucault: Beyond Structuralism and Hermeneutics* (Brighton: Harvester Press, 1982)

Gerstenfeld, P. B., Grant, D. R., and Chiang, C.P., 'Hate online: A content analysis of extremist websites' (2003) 3(1) *Analyses of Social Issues and Public Policy,* 29–44

Gibbons, L. J., 'No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace' (1997) 6 *Cornel Journal of Law and Public Policy*, 475-551

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

Goldsmith, J., 'The Internet, Conflicts of Regulation and International Harmonization', in Engel, C., and Keller, K. H., (Eds.) *Governance of Global Networks in the Light of Differing Local Values* (Baden-Baden: Nomos, 2000)

Goldsmith, J., 'Against Cyberanarchy' (1998) 65 (4) *University of Chicago Law Review*, 1199-1250

Goldsmith, J., and Wu, T., *Who Controls The Internet? Illusions of a Borderless World* (OUP, 2006)

Grimmelmann, J., 'Saving Facebook' (2009) 94 *Iowa Law Review*, 1149-1206

Grimmelmann, J., 'Virtual World Feudalism' (2009) 118 *Yale Law Journal Pocket Part,* 126

Grimmelmann, J., 'Virtual Worlds as Comparative Law' (2004) 49 *New York Law School Law Review*, 147-181

Greenberg, S., 'Threats, Harassment, and Hate On-Line: Recent Developments' (1997) 6 *Boston University Public Interest Law Journal,* 673, 675,680-684

Greenfield, A., *Everyware* (New Riders: Berkeley, 2006)

Hart, H.L.A., *The Concept of Law* (Oxford: Oxford University Press, 1961)

Hand, M., *Making Digital Cultures: Access, Interactivity, and Authenticity* (Hampshire: Ashgate, 2008)

Halder, D., and Jaishankar, K., 'Online Social networking and Women Victims', in Jaishankar, K., (Ed.) *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* (Boca Raton, FL: CRC Press, 2011) 301-320

Healy, D., 'Cyberspace and place: The Internet as middle landscape on the electronic frontier', in Porter, D., (Ed.) *Internet Culture* (NY: Routledge, 1997) 55-68

Heim, M., *The Metaphysics of Virtual Reality* (Oxford: OUP, 1993)

Hirschi, T., *Causes of Delinquency* (Berkeley: University of California Press, 1969)

Home Office, *Stalking—the solutions: A consultation paper* (London: Stationery Office, 1996) 1.2

Huberman, B.A., and Adamic, L.A., 'Growth dynamics of the World-Wide Web' (1999) 406 *Nature*, 450-457

Huang, P. H., and Wu, H., 'More Order without More Law: A Theory of Social Norms and Organizational Cultures' (1994) 10(2) *Journal of Law Economics & Organisation*, 390-406

Jenkins, P., *Beyond tolerance: Child pornography on the Internet* (New York: New York University Press, 2001)

Jewkes, Y., *Media and Crime: Key Approaches to Criminology* (Thousand Oaks: Sage Publications, 2004)

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

Johnson, D., and Post, D., 'Law and Borders—the Rise of Law in Cyberspace' (1996) 48 *Stanford Law Review*, 1368-1378

Joseph, J., 'Cyberstalking: An International Perspective', in Jewkes, Y., (Ed.) *Dot.Cons: Crime, Deviance and Identity on the Internet* (Collumpton: Willian, 2002) 105-125

Jordan, C. E., Quinn, K., Jordan, B., and Daileader, C. R., 'Stalking: Cultural, clinical and legal considerations' (2000) 38 (3) *Brandeis Journal of Family Law*, 513-579

Kang, J., 'Cyber-Race' (2000) 113 (5) *Harvard Law Review*, 1130-1209

Keleman, M., and Smith, W., 'Community and its 'virtual' promises, A critique of cyber libertarian rhetoric' (2001) 4 (3) *Information, Communication & Society*, 370-387

Keenahan, D., and Barlow, A., 'Stalking: A Paradoxical Crime of the Nineties' (1997) 2 (4) *International Journal of Risk, Security and Crime Prevention,* 291 - 300

Kerr, O. S., 'Criminal Law in Virtual Worlds' (2008) *University of Chicago Legal Forum*, 415-429

Koops, Bert-Jaap., et al, *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-Liners* (The Hague: TMC Asser Press, 2006)

Küpper, A., *Location-based services: fundamentals and operation* (Chichester, England; Hoboken, NJ: John Wiley 2005)

Lastowka, G. F., and Hunter, D., 'Virtual crimes' (2004) 49(1) *New York Law School Law Review*, 293–316

Lastowka, G. F., and Hunter, D., 'The Laws of the Virtual Worlds' (2004) 92 (1) *California Law Review*, 3-74

Lessig, L., *Code and other Laws of Cyberspace* (New York: Basic Books, 1999)

Lee, R. K., 'Romantic and electronic stalking in a college context' (1998) 4 *William & Mary Journal of Women and the Law*, 373–466

Li, C., and Bernoff, J., *Groundswell: Winning in a World Transformed by Social Technologies* (Boston: Harvard Business Press, 2008)

Lindenberg, S., 'Grounding Groups in Theory: Functional, Cognitive and Structural Interdependencies', in Lawler, E. J., (Ed.) *Advances in Group Processes* (Greenwich, CT: JAI Press, 1997) 281–331

Licklider, J. C. R., and Taylor, R. W., 'The computer as a communication device', (1968) Science and Technology Republished in SRC Research Report 61, Digital Equipment Corporation, 1990, 37-38 Available:

ftp://ftp.digital.com/pub/DEC/SRC/research-reports/SRC-061.pdf

Lockard, J., 'Progressive politics, electronic individualism and the myth of the virtual community', in Porter, D., (Ed.) Internet Culture (New York: Routledge, 1997) 219-231

Maple, C., Short, E., and Brown, A., 'Cyberstalking in the United Kingdom: An Analysis of the ECHO Pilot Survey' (National Centre for Cyberstalking Research, 2011)

Mayer-Schonberger, V., and Crowley, J., 'Napster's Second Life- the Regulatory Challenges of Virtual Worlds' (2006) 100 (4) *North Western University Law Review*, 1775, 1781

Mayer-Schonberger, V., 'The Shape of Governance: Analysing the World of Internet Regulation' (2003) 43 (3) *Virginia Journal of International Law* , 605-673

McEwan, T.E., Mullen, P.E., and MacKenzie, R., 'Anti-Stalking Legislation in Practice: Are we meeting community needs?' (2007) 14 (2) *Psychiatry, Psychology and Law*, 207-217

McKenna, K. Y. A., Green, A. S., and Gleason, M. E. J., 'Relationship formation on the Internet: What's the big attraction?' (2002) 58 (1) *Journal of Social Issues,* 9–31

McGuire, M., *Hypercrime: The New Geometry of Harm* (London: Routledge-Cavendish, 2007)

McGrath, M. G., and Casey, E., 'Forensic Psychiatry and the Internet: Practical Perspectives on Sexual Predators and Obsessional Harassers in Cyberspace'(2002) 30 (1) *The Journal of the American Academy of Psychiatry and the Law*, 81-94

Meloy, J.R., 'The psychology of stalking', in Meloy, J.R., (Ed.) *The Psychology of Stalking: Clinical and Forensic Perspectives* (NY: Academic Press, 1998) 1–23

Moore, R., Ducheneaut, N., and Nickell, E., 'Leveraging virtual omniscience: Mixed methodologies for studying social life in persistent online worlds' (2005) Workshop presented at the Games, Learning, and Society Conference, Madison WI, June 23-24, 2005

Miller, D., and Slater, D., *The Internet: an Ethnographic Approach* (Oxford/New York: Berg, 2000)

Murray, A. D., *The Regulation of Cyberspace* (Abingdon: Routledge-Cavendish, 2007)

Mullen, P. E., Pathe, M., and Purcell, R., *Stalkers and their Victims* (NY: CUP, 2000)

Murnion, S., and Healey, R.G., 'Modelling Distance Decay Effects in Web Server Information Flows' (1998) 30 (4) *Geographical Analysis*, 285-303

Nakhaie, M., Silverman, R., and LaGrange, T., 'Self-Control and Social Control: An Examination of Gender, Ethnicity, Class and Delinquency' (2000) 25 (1) *The Canadian Journal of Sociology*, 35-59

Oldenburg, R., *The Great Good Places* (NY: Paragon House, 1989)

Ogilvie, E., *Cyberstalking*: *Trends and Issues in Crime and Criminal Justice,* No. 166 (Canberra: Australian Institute of Criminology, 2000)

Paternoster, R., 'How much do we really know about criminal deterrence?' (2010) 100 *Journal of Criminal Law and Criminology*, 765-824

Perritt, H. H. Jr., 'Cyberspace Self-Government: Town Hall Democracy or Rediscovered Royalism?' (1997) 12(2) *Berkeley Technology Law Journal*, 413-475

Picker, R. C., 'Cybersecurity: of Heterogeneity and Autarky', in Grady, M. F., and Parisi, F., (Eds.) *The Law and Economics of Cybersecurity* (CUP, 2005) 115, 117

Preece, J., 'Etiquette Online: From Nice to Necessary' (2004) 47(4) *Communications of the Association of Computing Machinery,* 56–61

Post, D. G., 'Governing *Cyberspace: Law*' (2008) 24 (4) *Santa Clara Computer & High Technology Law Journal*, 883-913

Qualman, E., *Socialnomics: How Social Media Transforms the Way We Live and Do Business* (Hoboken, N.J.: Wiley, 2009)

Rawls, J., *A theory of justice* (Cambridge: Harvard, 1971)

Reed, C., *Making Laws for Cyberspace* (OUP, 2012)

Reed, C., 'How to Make Bad Law: Lessons from Cyberspace' (2010) 73(6) *Modern Law Review*, 903-932

Reed, C., 'Why must you be mean to me? Crime and the Online Persona' (2010) 13 (3) *New Criminal Law Review: An International and Interdisciplinary Journal,* 485-514

Reidenberg, J. R., 'Governing Networks and Rule-Making in Cyberspace' (1996) 45 *Emory Law Journal*, 911-929

Reid, E., 'Virtual Worlds: Culture and Imagination' in Jones, S. G., (Ed.) *Cyber society: Computer-Mediated Communication and Community* (London: Sage, 1995) 164-183

Reid, E., 'Hierarchy & Power: Social Control in Cyberspace', in Kollock, P., and Smith, A., (Eds.) *Communities in Cyberspace* (London: Routledge, 1999) 107–133

Rheingold, H., *The virtual Community: Homesteading on the Electronic Frontier* (2nd Edition) (London: MIT Press, 2000)

Risch, M., 'Virtual Rule of Law' (2009) 112 (1) *West Virginia Law Review*, 1-50

Rothchild, J., 'Protecting the Digital Consumer: The Limits of Cyberspace Utopianism' (1999) 74 (3) *Indiana Law Journal*, 893-998

Salter, M., and Bryden, C., 'I can see you: Harassment and Stalking on the Internet' (2009) 18 (2) *Information & Communications Technology Law*, 99-122

Schrock, A., and Boyd, D., 'Problematic Youth Interaction Online: Solicitation, Harassment, and Cyberbullying', (2011) in Wright, K.B., and Webb, L. M., (Eds.) *Computer-Mediated Communication in Personal Relationships* (New York: Peter Lang)

Schaap, F., *The Words that took us there: Ethnography in a Virtual Reality* (Piscataway NJ: Transaction Publishers, 2002)

Seto, K. W., 'How Should Legislation Deal With Children as the Victims and Perpetrators of Cyberstalking?' (2002) 9 *Cardozo Women's Law Journal*, 67, 73-74

Shiode, N., and Dodge, M., 'Spatial analysis on the connectivity of information space' (2000) 8 (2) *Theory and Applications of GIS*, 17-24

Shaw, D. B., *Technoculture: The Key Concepts* (New York: Berg, 2008)

Simpson, B., 'What happens online stays online? Virtual punishment in the real world' (2011) 20 (1) *Information & Communications Technology Law*, 3-17

Smith, R., Grabosky, P., and Urbas, G., *Cybercriminals on Trial* (Cambridge: CUP, 2004)

Spitzberg, B. H., and Hoobler, G., 'Cyberstalking and the technologies of interpersonal terrorism' (2004) 4(1) *New Media & Society*, 71–92

Spender, D., *Nattering on the Net* (North Melbourne: Spinifex Press, 1995)

Stoup, P., 'The Development and Failure of Social Norms in Second Life' (2008) 58 (2) *Duke Law Journal*, 311-344

Stillman, L., and McGrath, J., 'Is it Web 2.0 or is it Better Information and Knowledge that We Need?' 61 (4) *Australian Social Work*, 421–428

Suzor, N., 'Order Supported by Law: The Enforcement of Rules in Online Communities' (2012) 63 (2) *Mercer Law Review*, 523-595

Sykes, G. M., and Matza, D., 'Techniques of Neutralization: A Theory of Delinquency' (1957) 22 (6) *American Sociological Review*, 664- 670

Taylor, T. L., *Play between Worlds: Exploring Online Game Culture* (Cambridge: MIT Press, 2006)

Tyler, T.R., *Why People Cooperate* (Princeton: Princeton University Press, 2011)

Tyler, T.R., and Blader, S., *Cooperation in groups: Procedural justice, social identity, and behavioral engagement* (Philadelphia: Psychology Press, 2000)

Tyler, T.R., Degoey, P., and Smith, H., 'Understanding why the justice of group procedures matters: A test of the psychological dynamics of the group-value model' (1996) 70 (5) *Journal of Personality and Social Psychology*, 913-930

University of Modena and Reggio Emilia Modena Group on Stalking, *Protecting Women from the New Crime of Stalking: a comparison of legislative approaches within the European Union* (University of Modena and Reggio Emilia Modena Group on Stalking, 2007)

Valetk, H. A., 'Cyberstalking: Navigating a Maze of Laws' (2002) 228 *New York Law Journal,* 1-5

Vickery, G., and Wunsch-Vincent, S., *Participative Web and User-Created Content: Web 2.0, Wikis and Social Networks* (Paris: OECD, 2007)

Walther, J., 'Group and interpersonal effects in international computer-mediated communication' (2007) 23 (3) *Human Communication Research,* 342-369

Wall, D., 'Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime' (2008) 22(1) *International Review of Law, Computers and Technology*, 45-63

Wall, D., 'Cybercrime and the Culture of Fear: Social science fiction(s) and the production of knowledge about cybercrime' (2008/11) 11(6) *Information, Communication & Society,* 861–884

Wall, D., *Cybercrimes: The Transformation of Crime in the Information Age*. (Cambridge, UK: Polity, 2007)

Wall, D., 'The Internet as a Conduit for Criminals', in Pattavina, A., (Ed.) *Information Technology and the Criminal Justice System* (Thousand Oaks, CA: Sage, 2005) 77-98

Wall, D., 'Digital Realism and the Governance of Spam as Cybercrime' (2005) 10 (4) *European Journal on Criminal Policy and Research*, 309-335

Wall, D., and Williams, M., 'Policing diversity in the digital age: Maintaining order in virtual communities' (2007) 7 (4) *Criminology and Criminal Justice*, 391-415

Wellman, B., Boase, J., and Chen, W., 'The Networked Nature of Community: Online and Offline' (2002) 1 (1) *IT & Society,* 151-165

White, B. A., *Second Life: A Guide to Your Virtual World* (QUE, 2007)

Whitty, M.T., and Johnson, A.N., *Truth, Lies and Trust on the Internet* (Hove and New York: Routledge, 2009)

Wittel, A., 'Toward a network sociality' (2001) 18 (6) *Theory, Culture & Society,* 51-76

Williams, M., *Virtually Criminal: Crime, deviance and regulation online* (London: Routledge, 2006)

Wilson, J. Q., and Herrnstein, R. J., *Crime and Human Nature* (Simon and Schuster: New York, 1985)

Wu, T.S., 'Cyberspace Sovereignty? The Internet and the International System' (1997) 10 (3) *Harvard Journal of Law and Technology*, 647-666

Wu, T.S., *Who Controls the internet: Illusions of a Borderless World* (OUP, 2006)

Wykes, M., 'Constructing Crime: Culture, Stalking, Celebrity and Cyber Crime' (2007) 3 (2) *Media and Culture*, 158-174

Yee, N., 'The Psychology of Massively Multi-User Online Role-Playing Games: Motivations, Emotional Investment, Relationships and Problematic Usage', in Schroeder, R., and Axelson, A., (Eds.) *Avatars at Work and Play: Collaboration and Interaction in Shared Virtual Environments* (Springer: Netherlands, 2006) 187-207

Ybarra, M. L., Mitchell, K., Finkelhor, D., and Wolak, J., 'Internet prevention messages: Are we targeting the right online behaviors?' (2007) 161 (2) *Archives of Pediatric and Adolescent Medicine,* 138–145

Ybarra, M. L., and Mitchell, K., 'How risky are social networking sites? A comparison of places online where youth sexual solicitation and harassment occurs' (2008) 121 (2) *Pediatrics,* 350-357