BILETA

14th BILETA Conference: "CYBERSPACE 1999: Crime, Criminal Justice and the Internet".

Monday, March 29th & Tuesday, March 30th, 1999.
College of Ripon & York St. John, York, England.

On the Politics of Policing the Internet: Striking the right balance

David S. Wall
Cyberlaw Research Unit, Centre for Criminal Justice Studies, Faculty of Law, University of Leeds

Abstract

Over the past decade, the concept of cyberspace has developed from science fiction into a socially constructed reality. As a political economy of information capital develops, the intellectual 'land grab', that is currently taking place for control over cyberspace, is generating new distinctions between acceptable and deviant behaviour, as well as creating new public demands for regulation. Many activities are becoming labelled as criminal and now sit next to those behaviours for which a remedy is found in criminal law. New types of risk communities now accompany the old.

The above situation has created some interesting, but often contradictory scenarios. On the one hand there are some increasing public concerns over the inability of recognised authorities to regulate behaviour in cyberspace. And yet on the other hand, there are quite clear examples of scare-mongering by the burgeoning cyber-crime industry. Characteristic of the latter is the failure to dissagregate between the potential and actual harms that occur in, or as the result of, cyberspace, thus fuelling the public panic, either to achieve a new commercial market or to secure public funds.

This paper will explore some of the complex issues surrounding our (lack of) knowledge about cybercrimes and how they may "policed". It will, firstly, look briefly at why the cyberspace needs to be policed, especially at what we currently understand as a "cybercrime" and will comment upon who are the victims and who are the offenders. The second part will look at the strategies that exist for the policing of cyberspace and indeed, who is actually policing it. The third part will offer some conclusions.

The internet-based communications industry has, during the 1990s, rapidly developed into the strategic thinking of both Governments, their component institutions and also the major international companies. But along with the extremely desirable aspects of virtual life come the darkside and it is with this in mind that a rather paradoxical situation is emerging. On the one hand, it is now quite clear that the Internet really does have the capability to transcend economic, political, geographical, social and even racial and gendered boundaries that the early commentators had predicted (Barlow, 1993, Rheingold, 1994, Saradar and Ravetz, 1996: 1).

On the other hand, although the mass media would have us believe otherwise, the anarchy that was predicted by those who favoured early regulation has not materialised, and the cyberspace which has been created by the Internet is remarkably ordered considering its sheer size in terms of the large numbers of individuals involved and also the breadth of their involvement (Davies, 1996). So, we either have a case of exaggerated claims, or there is some mechanism that is already operating to

police or regulate cyberspace. In fact it will be suggested later in this article that the answer is a bit of both. But it is with this paradox in mind that this article will explore the policing of cyberspace. Clearly the policing of the Internet is about more than just simply enforcing the law, rather it is about regulating the behaviour of Internet users. And by engaging the issue at the point where the debate over policing the Internet shifts from legal regulation to the broader issue of governance, the article will also seek to establish exactly who is regulating the behaviour of whom within the powerplay that is currently taking place to control cyberspace. Furthermore, it will be suggested that a fairly effective system of multi-tiered policing has already developed within cyberspace and that this model will best provide the basis for any future developments in the policing of the medium. Of particular importance is the view that any such developments should include a framework of accountability that would incorporate a series of checks and balances to protect civil liberties against the expression of various political, moral and commercial power interests that are currently vying for control over cyberspace.

So, this article is essentially a topographical exercise that is designed to map out the contours of policing the Internet. The first part will look briefly at why the cyberspace needs to be policed, especially at what we currently understand as a "cybercrime", who are the victims and who are the offenders. The second part will look at who is actually policing cyberspace, and the third part will offer some conclusions.

What is the problem, and who or what needs policing?

The Internet has impacted upon human activities (Escobar, 1996); Loader, 1996; Reingold, 1994; Barlow, 1993; Wall; 1997) in two main ways. Firstly, it has acted as a vehicle for the further facilitation of existing activities. Secondly, it has created an environment, a cyberspace, which has facilitated the creation of entirely new types of activities which are largely free of traditional and terrestrial constraints. It is along these same lines that the Internet has also facilitated the development of undesirable behaviours or harms. With regard to the former we find that the Internet has, for example, enabled the execution of fraudulent activity or has enabled paedophiles to conduct their undesirable practices. With regard to the latter, we see the development of new types of harmful activities which are novel in so far as they lie outside our existing experiences and demand both new forms of understanding and also legal responses. To name a few examples, we see the creation of new forms of obscenity through computer generated images (pseudo-photographs), and the development of new forms of appropriation such as the theft of visual imagery that possesses a high intellectual property value and the waging of information warfare via the illegal invasion of computer space and the destruction of materials within it.

A more systematic categorisation suggests that there are four main groups of behaviour relating to the Internet that are currently causing concern. They are obscenity, trespass, theft and violence, and each group illustrates a range of activities rather than actual offences (Wall, 1999).

Cyberobscenity refers to the trade of obscene materials within cyberspace. The cyberobscenity debate is very complex. Its newsworthiness has not only driven the debate over the regulation of cyberspace, but its resolution is also marred by both normative perceptions and definitional variations across legal jurisdictions. In Britain, for example, individuals regularly consume images that might be classed as obscene in many middle-Eastern countries. And yet, what individuals class as obscene in the United Kingdom is often acceptable to the citizens of more permissive countries, such as some of those in Scandinavia.

Cybertrespass (unauthorised access to data) relates to the crossing of established boundaries into spaces over which control has already been established. In its mildest form, cybertrespass can be little more than an irritating intellectual challenge resulting in a harmless trespass, but at its worst, it

is full blown information warfare between social groups or even nation states. Somewhere between these positions falls the cybervandal, spy and terrorist.

Cybertheft relates to a range of different types of acquisitive harm that can take place within cyberspace. At one level are the more traditional patterns of theft, such as the fraudulent use of credit cards and (cyber)cash. Of particular concern is the increasing potential for the raiding of online bank accounts. There have already been incidents of this activity. At another level are those acts which will cause us to reconsider our understanding of property and therefore the act of theft, such as cyberpiracy (the appropriation of intellectual properties).

Cyberviolence describes the violent impact of the cyberactivities of another upon an individual or social grouping. Whilst such activities do not have to have a direct physical manifestation, the victim nevertheless feels the violence of the act and can bear long-term psychological scars as a consequence. The activities referred to here range from cyberstalking (Ellison and Akdeniz, 1998) to hate speech and bomb-talk.

These four categories demonstrate the range of cyberactivities that are causing concern and are leading to demands for the greater regulation of cyberspace. Their resolution is not simply a matter of engaging specific bodies of criminal law. The issue is rather more complex as the harms are defined by a complex combination of normative, political and legal values. The issue is further complicated by the following four factors.

Firstly, many definitions of offence and offender are being forged by the fight, or "intellectual land grab" (Boyle, 1996: 125), that it taking place for control over cyberspace. Of particular importance here is the increasing level of intolerance that is being demonstrated by "the powerful" towards certain "risk groups" that they perceive as a threat to their interests. Such intolerance tends to mould broader definitions of deviance. But the definitions of deviance are not so simply one-sided, as Melossi has argued that definitions of crime and deviance arise, not only from the social activity of élite or power groups, but also from that of "common members" of society and offenders themselves: "the struggle around the definition of crime and deviance is located within the field of action that is constituted by plural and even conflicting efforts at producing control" (Melossi, 1994: 205). Secondly, there is often some confusion as to whether or not the harms fall under civil or criminal laws, and to complicate matters further, some harms will be classed as criminal in some jurisdictions and civil in others. Thirdly, there is a degree of confusion over who the victims are and how they are being victimised. Not only can victims vary from individuals to social groupings, but the (cyber) harms done to them can range from the actual to the perceived. In cases such as cyberstalking or the theft of cybercash, the victimisation is very much directed towards the individual. However, in other cases the victimisation is more indirect, such as with cases of cyberpiracy or cyberspying/ terrorism. Furthermore, as has been found to be the case with the reporting of white-collar crimes, it is likely that many victims of cybercrimes, be they primary or secondary victims, may be unwilling to acknowledge that they have been a victim, or it may take them some time to realise it. Alternatively, where the victimisation has been imputed by a third party upon the basis of an ideological, political, moral, or commercial assessment of risk, the victim or victim group may simply be unaware that they have been victimised or may even believe that they have not, such is the case with some forms of pornography. Fourthly, the cyberoffenders are fairly atypical in terms of traditional criminological expectations, which problematises the identification of the offender. Although itself contested, the debate over the policing of traditional crimes has tended to be located within the analysis of working class sub-cultures or the underclass; offenders in cyberspace are middle class, without criminal records, often expert and skilled and motivated by a variety of financial and non-financial goals.

So, what this brief analysis suggests is that the demands for the regulation of the Internet vary considerably. Some behaviours and harms are clearly covered by agencies related to existing criminal and civil law, others however, are more complicated and can only be dealt with by other bodies and means. In both cases, some form of check or test is required in order to establish that the

harms are real and not hypothetical, whether it be in the enforcement of law or during the formulation of policy. The following section will look at how, and by whom, the Internet is currently being policed.

How is cyberspace currently being policed?

When exploring the policing of the Internet, it is important to distinguish between bodies which seek to promote or protect norms and values, and those bodies which seek to enforce them. The former group include policy-making groups and legislators at both a national level and at an international level in the case of the United Nations and the European Union (Walker and Akdeniz, 1998). The mandate of both is derived, directly or indirectly, from the formal democratic process. This group also includes the various pressure groups which represent specific interests and who lobby in order to further their cause or protect the interests of their members. In contrast with the legislators, their mandate is drawn from their support of a range of specific moral or political issues. Such pressure groups range from user groups, like Cyber-Rights and Cyber-Liberties, to groups of Internet Service Providers such as the Internet Service Providers Association which seeks to "promote the interests of Internet Service Providers in the UK...". Finally, there are the various organisations which are actively involved in the policing of cyberspace and which exist to enforce the norms of the former groups through various management strategies which effect a policing function. In practice it is often hard to disaggregate the two, but the following discussion will focus upon the latter group.

Currently, there are four main levels at which policing activity takes place within cyberspace: the Internet users themselves; the Internet Service Providers; state-funded non-public police organisations: and state-funded public police organisations. At each level the organisations or groups involved will also tend to find an expression in transnational forms (Sheptycki, 1998a: 485; 1998b: 17) because of the global nature of the Internet. This reflects the "organisational bifurcation" (Reiner, 1992b: 761) or "spatial polarisation" (Johnston, 1993: 56; Jones and Newburn, 1998: 260) that is also taking place within the sphere of terrestrial policing.

The *Internet Users* are the largest group of individuals to be inducted into policing the Internet. Within the user group are a number of sub-groups which have formed around specific issues in order to police web sites that offend them. Largely transnational in terms of their membership and operation, these groups tend to be self-appointed and possess neither a broad public mandate nor a statutory basis, consequently they lack any formal accountability for their actions which themselves may be intrusive or even illegal. However, they would seem to possess a fairly potent force, and a number of visible examples of virtual community policing have already occurred. In addition to the various complaint "hotlines" and the development of software to screen out undesirable communications (Uhlig, 1996a), there are a few recorded netizen groups which have attempted to organise Internet users. The Internet Rapid Response Team (IRRT), for example, came to prominence when an e-mail message advertising a collection of child pornography, which carried a New York address, was received by thousands of Internet users all over the world (Uhlig, 1996a). It's response was to "spam" the New York Police with calls for an immediate investigation. The IRRT is a voluntary group which polices the Internet to remove offensive material. The philosophy of the IRRT is that "it is up to Internet users as much as anyone else to react quickly when something like this happens" (Uhlig, 1996a).

Another netizen group which actively police cyberspace are the CyberAngels, a 1000 strong organisation of net users who are also based, as their name suggests, along the Guardian Angel model. Divided into "Internet Safety Patrols", they operate in the four main areas of the Internet: Internet Relay Chat (IRC), Usenet, World Wide Web (WWW), and the net services provided by the largest US ISP, America Online (AOL). Their function is to actively promote, preserve and protect netiquette which "is the collection of common rules of polite conduct that govern our use of the

Internet". Importantly, they claim the right to question what they encounter, and they argue that they have a civil, legal and human right to bring it to the attention of the proper authorities. Their mission statement says that they are dedicated to fighting crime on the Internet "where there are clear victims and/or at-risk users", they seek to protect children from online criminal abuse, they give support to online victims and advise them upon how to seek a remedy, seek out materials that will cause harm, fear, distress, inconvenience, offence or concern, "regardless of whether it is criminal or not".

Groups like the IRRT and CyberAngels perform a broadly ranging policing function, but other groups of netizens dedicate themselves to specific types of cyberharm, the most common being child pornography. Phreakers & Hackers (UK) Against Child Porn (PH(UK)ACP), for example, claim not to be vigilantes, but aim to track down offensive sites and interfere with their operation. A similar group are Ethical Hackers Against Porn (EHAP) who like, PH(UK)ACP, "want to stop child exploitation" and claim to work in loose co-operation with government and local officials, even though they admit to "using unconventional means to take down the worst, most unscrupulous criminals known". One of the most interesting paradoxes that currently exists with regard to the issue of child pornography on the Internet is the large amount of support given to efforts to counter it by the "mainstream" pornographers who wish to distance themselves from the issue, but also seek to legitimise their own activities.

The Internet Service Providers: The ISPs have a rather fluid status which arises from the fact that although they are physically located in a particular jurisdiction, they tend to function in a transnational way. The moral panic (Cohen, 1972; Chandler, 1996: 229) surrounding the Internet during the mid-1990s over the perceived threat of widespread pornography (Wall, 1997), and the subsequent threats of legal action (Uhlig, 1996b), has forced Internet Service Providers to consider the possibility of controlling some of the activities that are taking place on their servers: especially the news discussion groups. In August 1996, the former Science and Technology Minister, warned that "in the absence of self-regulation, the police will inevitably move to act against service providers as well as the originators of illegal material" (Uhlig,1996b). This statement was quickly followed by a letter sent to Internet Service Providers by the Metropolitan Police Clubs and Vice Unit, warning that they could be liable for any illegal materials that were found to have been disseminated on their servers. Their response in September 1996 was to promote "SafetyNet", a mix of "self-ratings", classification, user control and public reporting plus law enforcement action. SafetyNet was jointly endorsed by the Metropolitan Police, Department of Trade and Industry (DTI), Home Office and the associations of the Internet Service Providers; the Internet Service Providers Association and the London Internet Exchange (Uhlig, 1996c). In December 1996, SafetyNet became the Internet Watch Foundation (IWF) (Tendler, 1996). Since its formation, the standing of the Internet Watch Foundation has increased and it has become the quasi-public face of Internet regulation in the UK. One of its functions is to overview the use of the Internet and bring to the attention of ISPs any illegal materials that are reported to its hotline. Between December 1996 and November 1997 the IWF received 781 reports, mostly by e-mail, which covered 4324 items (mostly on newsgroups). Action was taken with regard to 248 reports, and the greater majority, 85 per cent, related to child pornography, the eradication of which is one of the objectives of the Foundation.

The Internet Watch Foundation has a mandate from both the ISPs and also the UK government, but Akdeniz argues that the IWF does not command a defined body of public support, especially for its Internet rating system, which has had very little public discussion. However, it is probably the case that were the IWF to canvass public opinion over the issues such as child pornography, then such public support would be considerable. Of considerable further concern is the fact that the Internet Watch Foundation retains the status of being a private organisation with a very public function and as such lacks the structures of accountability that are normally associated with organisations that have a public function.

Although the legal status of ISPs as a publisher is now quite widely acknowledged, their liabilities vary under various bodies of law and have yet to be fully established (Edwards and Wealde, 1997;

Lloyd, 1997; Rowland and Macdonald, 1997). Consequently, ISPs tend to tread fairly carefully and be responsive to requests for co-operation. Not only are they very wary of their potential legal liabilities, but also it is probably fair to say that they are fearful of any negative publicity which might arise from their not being seen to act responsibly. Interestingly, the police themselves also appear to be fairly uncertain about their general position with regard to the prosecution of ISPs. Whilst they have continued to warn the ISPs about possible prosecutions since 1996, none of the promised prosecutions has been brought against Internet Service Providers in the UK. The general rule of thumb that appears to be adopted across many jurisdictions is that liability tends to arise when the ISP fails to remove offensive material, whether it be obscene or defamatory, provided it has been brought to their attention following a complaint.

There is a degree to which the ISPs are organised at a transnational level, for example, the Commercial Internet eXchange, the Pan-European Internet Service Providers' Association (EuroISPA) and Internet Service Providers' Consortium (mainly USA). However these organisations tend to be more involved with technical and commercial issues that are germane to ISPs than specifically with the self-policing of ISPs.

State-Funded Non-Public Police Organisations: The next level of policing involves state agencies, but these are bodies not normally perceived as "police" nor are they given the title "police". For example, some governments, such as Singapore, China, Korea and Vietnam, have actively sought to control their citizen's use of the Internet, either by forcing users to register with governmental monitoring organisations or by directly controlling Internet traffic coming into their countries through government-controlled Internet Service Providers (Center for Democracy and Technology, 1996; Caden and Lucas, 1996; Standage, 1996; Grossman, 1996b).

Within Europe, Germany has set up a regulatory agency, the Internet Content Task Force, and has passed new telecommunications laws requiring Internet Service Providers to provide a back door so that security forces can read user's electronic mail if necessary (Grossman, 1996b). The Internet Content Task Force also has powers to force German Internet Service Providers to block access to certain materials, such as the Dutch site "xs4all". A similar organisation is currently being set up by the French government, which has also passed legislation to set up a central regulatory agency (Grossman, 1996b).

In the United States, a number of state funded non-public police organisations have become involved in policing the Internet. In part, this is inevitable because the trans-jurisdictional nature of Internet traffic involves federal rather than provincial state agencies, however such a development does fit in with the US strategy towards the Internet. The United States Postal Service, for example, was instrumental in investigating offences of pornography in the case of *United States of America v. Robert A. Thomas and Carleen Thomas*, after a computer hacker from Tennessee filed a complaint about the contents of a bulletin board containing obscene materials (Byassee,1997: 205). The case was subsequently investigated by a United States postal inspector. In another incident the US Securities and Exchange Commission, which was "anxious about the spread of cyberfraud", brought a case against a publicly-traded company for allegedly conducting a fraud through the Internet. The Commission noted that it anticipated that it "will be addressing this kind of conduct on the Internet more frequently" in the coming millennium (Pretzlik, 1996).

In addition to involving state funded non public police organisations, the US government have tried, with varying degrees of success, to introduce legal measures and develop technological devices to regulate cyberspace in order to "protect the interests of US industry" (Reno, 1996). For example, the V-chip technology, which is designed to filter out violence or pornography, and the "Clipper Chip" which is an "escrowed encryption system" that provides the government with codes to unscramble encrypted files (Akdeniz, 1996: 235-261; Post, 1995: 8; Sterling, 1994; Sussman, 1995: 54). Since the impact of many of these measures is also to curb individual freedom of communication, it is therefore not surprising that much of the debate over Internet regulation has revolved around the

First Amendment of the United States Constitution, especially during the legal challenge to the Communications Decency Act 1996.

An interesting example of a hybrid state-funded non public police organisation in the USA is the Computer Emergency Response Team (CERT), based at Carnegie Mellon University in Pittsburgh, USA. Unlike the UK's IWF, CERT is based within a public institution, however it appears to be funded by mainly private sources, but like the IWF, it has a public function. CERT exists to combat unauthorised access to the Internet, and 15 programmers log reported break-ins and carry out the initial investigations. Where security breaches are found to be too complicated to deal with in-house, they are farmed out to an unofficial "brain trust" (Adams, 1996).

*State Funded Public Police Organisations***:** The final group of organisations which are involved in policing the Internet are the state funded public police organisations whose formal status allows them to draw upon the democratic mandate of government. They tend to be organised either locally or nationally, depending upon the jurisdiction. However, whilst they tend to be located within the nation state, they are nevertheless joined by a tier of transnational policing organisations, such as Interpol, whose membership requires such formal status.

In the United Kingdom, the public police are mainly organised locally, but there also exist national police organisations that deal with the collection of intelligence and the investigation of more organised crime. Within the local bodies, several specialist individual or groups of police officers monitor the Internet (Davies, 1998). For example, a computer crime unit was established by the Metropolitan Police and a smaller, but similar, unit was set up by the Greater Manchester Police. Elsewhere, officers in the West Midlands Police and the Metropolitan Police Clubs and Vice Unit have used the Internet to collect intelligence about offences and offenders relating to the types of crime under their particular responsibility. At a national level, the National Criminal Intelligence Service (NCIS) has taken on the responsibility for providing intelligence on serious offences such as child pornography which cross both force and also international boundaries. From April 1998, the investigation of such offences came under the auspices of the National Crime Squad, a role that was previously held by the various regional crime squads. However, there does yet appear to be a British equivalent to the US Federal Bureau of Investigation's National Computer Crime Squad.

The emphasis to date upon the creation of specialist police units, whether local or national, raises the question as to the extent to which the public police as whole should integrate the policing of cyberspace within their "normal" functions (see Wall, 1997: 223-229). Clearly, it is almost certain that the incidence of cybercrimes will rise considerably as the population of cyberspace increases and there is an expansion of range of activities carried out within it. But whilst there is an argument that the state funded public police forces operate within existing (albeit contested) structures of accountability, it is highly likely that the public police will not become involved in the "patrolling" of cyberspace, or for that matter in the actual investigation of most cybercrimes. This is because of the largely private nature of the domain, because of the deeply entrenched and traditional nature of police work, and because of the sheer cost to the public purse that would be involved. Yet it is still likely to be the case that the public police will still perform an important gatekeeping function by being the first point of contact for members of the public against whom many of the cybercrimes have been committed. As such the public police will nevertheless have a role to play in the policing of the Internet. This highlights the need for the public police need to undergo some training in order to be aware of the various issues so that, on the one hand, they understand when, or indeed when not, to become involved, but also which body has responsibility for the various types of harm.

Conclusions: Getting the right balance

These are *early days in the life and times of cyberspace - too early to start predicting its full impact*

upon society with any degree of certainty, especially as the initial power-play for control over it is still taking place. It is quite clear that the benefits of the Internet have to be protected from the harms that could occur, but achieving this task is going to be very difficult because attempts by one group to curb the specific behaviours of another are not going to be well received, and the success of the operation will depend upon which group has the stronger mandate. It is also quite clear from the preceding discussion that *a multi-tiered system of policing is already developing which is largely based upon self-regulation by its netizens and the Internet Service Providers*. Such a system is not only a far more workable proposition than external regulation, which would be unpopular and very impractical, but it would also be much less costly. This approach was largely endorsed by a recent European Commission report on legal aspects of computer-related crime (Seiber, 1998; Walker and Akdeniz, 1998), though it went on to argue that for it to be effective there also needed to be in place an infrastructure of international agreements over the boundaries of acceptable and non-acceptable activities which take due account of fundamental civil liberties.

This latter point raises one of the main concerns with the self-policing model. Not only does *it presently tend to operate upon a self-appointed mandate*, but *it currently lacks formal mechanisms of accountability*. So, *the principle of self-policing is inherently limited in scope and has a fairly low ceiling of efficacy, after which the various higher levels of policing have to be invoked in order to resolve the situations which self-regulation fails to resolve*, does not apply to, or is not applied (Walker, 1997: 28; Wall, 1997: 222). Inevitably, the policing functions will be split between all of the levels of policing delineated in this paper (Wall, 1997: 224). The pluralistic model of policing the Internet that is described here combines elements of both public and private models of policing. It also reflects the increasing plurality of policing in high modernity at both a national and transnational level (Sheptycki, 1998).

In the final analysis, it is important to keep the issue of cybercrimes in perspective as there currently exist number of processes which have led to the problem being overstated, especially with regard to pornography. These claims raise a number of important issues.

First, if these estimates are accurate, then we must ask *why then are there not more cybercrimes*, why are they not more serious and why, for the most part, does the system clearly seem to police itself to the degree that it does? We must assume that these estimates and concerns largely relate to the potential harms that can be inflicted by cybercrimes and which do not necessarily translate into actual harms. Similar, say, to the advent of the motor car, just as not all drivers turned out to be drunks or road-ragers, so not all netizens are pornographers or paedophiles.

Secondly, there is some evidence to suggest that *much of the rhetoric regarding the extent of cybercrimes has been deliberately overblown* in order to draw funding for security and policing organisations. Duncan Campbell, believes that the case of the hackers, Bevan and Pryce (a schoolboy), revealed that "oversold threats" regarding the implications of breaches of security into major USA defence computers won funding from Congress (Campbell, 1997: 2). Bevan, for example, was accused by US military sources as being "a greater threat to world peace than Adolf Hitler" (Gunner, 1998: 5). The truth was subsequently found to be much less dramatic. However, the new funding led to the development of new military and intelligence "infowar" units, which have subsequently sold their security services to private corporations.

Finally, *a great danger arising from overstatement is that the (cyber)behaviours which have become labelled as deviant then become the subject of formal regulation without a complete analysis of their impact, implications or extent*. A graphic example of this process emerged following the moral panic over obscenity during the mid-1990s. A solution, in the form of the now-compromised (US) Communications Decency Act 1996, was sought before the problem had been properly identified (Wallace and Mangan, 1996: 174; Akdeniz, 1997: 1003).

In the not too distant future it is highly likely that many of the undesirable behaviours that were

described earlier will simply be worked out of the system, in that the victims and victim groups will find a way of regulating the behaviour. Alternatively, the behaviour may simply cease to be popular any more - a passing fad which ceases to be exciting or is replaced by more exciting, legitimate Internet usage. Moreover, it may also be the case that developments in technology will simply eradicate the problem, either by deliberate design, for example, through more secure communications, encryption and firewalling, or as a by-product or knock-on effect. Nevertheless, at the end of the day we shall be left with a series of new types of "criminal" behaviour, which will continue to challenge our traditional understandings of crimes, deviancy and the anti-social and the way that we police them. Our experience to date strongly suggests that we do not need new wholly forms of regulation or policing, but rather we need to adapt, develop and build upon those which exist already.

References

Adams, J. A. (1996) "Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet" 12 *Santa Clara Computer and High Technology Law Journal* 416.

Akdeniz, Y. (1996) "Computer pornography: a comparative study of US and UK obscenity laws and child pornography laws in relation to the Internet" 10 *International Review of Law, Computers and Technology* 235-261.

Akdeniz, Y. (1997) "Governance of Pornography and Child Pornography on the Global Internet: A Multi-Layered Approach", in Edwards, L. and Wealde, C., (eds) *Law and the Internet: Regulating Cyberspace* (Oxford, Hart Publishing, 1997).

Akdeniz, Y. (1997) "The battle for the Communications Decency Act 1996 is over", 147 *New Law Journal* 1003.

Akdeniz, Y. (1998) "Who Watches the Watchmen: Part II: Accountability and Effective Self-Regulation in the Information Age" <http://www.cyber-rights.org/watchmen-ii.htm>.

Arthur, C. (1996) "New crack-down on child porn on the Internet" *The Independent*, 23 September.

Barlow, J.P., (1993) "Selling Wine Without Bottles: The Economy of Mind on the Global Net" <http://www.eff.org/pub/Publications/John_Perry_Barlow/HTML/idea_economy_article.html>.

Boyle, J. (1996) *Shamans, Software and Spleens: Law and the Construction of the Information Society* (Harvard University Press, Cambridge, Mass).

Byassee, W. S., "Jurisdiction of Cyberspace: applying real world precedent to the virtual community" (1997) 30 *Wake Forest Law Review* 205.

Caden, M. L. and Lucas, S. E. (1996) "Accidents on the Information Superhighway: on-line liability and regulation" 2(1) *Richmond Journal of Law & Technology*.

Campbell, D. (1997) "More Naked Gun than Top Gun" *The Guardian* (OnLine), 27 November p. 2.

Center for Democracy and Technology (1998) "Regardless of Frontiers: Protecting the Human Right to Freedom of Expression on The Global Internet" (Washington, Global Internet Liberty Campaign).

Center for Democracy and Technology (1996) "Silencing the New: The Threat to Freedom of Expression On-Line" <gopher://gopher.igc.apc.org:5000/00/int/hrw/expression/7>.

Chandler, A. (1996) "The changing definition and image of hackers in popular discourse" 24

International Journal of the Sociology of Law 229.

Cohen, S. (1972) *Folk Devils and Moral Panics* (Paladin, London).

Crawford, A., *Crime Prevention and Community Safety*(Longmans, Harlow, 1998).

Davies, D.J. (1998) " Criminal Law and the Internet: the investigator's perspective" [1998] *Criminal Law Review*, Special Issue, December.

Davies, S. (1996) "Make it safe, but keep it free" *The Independent*, 4 September.

Edwards, L., and Wealde, C. (1997) (eds) *Law and the Internet: Regulating Cyberspace* (Oxford, Hart Publishing, 1997).

Ellison, L., and Akdeniz, Y. (1998) " Cyber-stalking: the Regulation of Harassment on the Internet" *Criminal Law Review*, December.

Escobar, A. (1996) "Welcome to Cyberia: Notes on the anthropology of cyberculture", in Saradar, Z. and Ravetz, J.R., (eds.) (1996).

Giddens, A. (1990) *The consequences of modernity* (London, Polity Press).

Grossman, W. (1996a) "A grip on the new" 496 *Electronic Telegraph*, 1 October.

Grossman, W. (1996b) "A grip on the new" (1996) 496 *Electronic Telegraph*, 1 October.

Gunner, E. (1998) "Rogue hacker turned legit code-cracker" *Computer Weekly*, 7 May.

Johnson, L., *The Rebirth of Private Policing* (London, Routledge, 1992).

Johnston, L. (1993) "Privatisation and protection: spatial and sectoral ideologies in British policing and crime prevention" 56 *Modern Law Review* 771.

Jones, T., and Newburn, T., (1998) *Private Security and Public Policing* (Oxford, Clarendon Press).

Leong, G., " Computer Child Pornography - the liability of distributors?" [1998] *Criminal Law Review* Special Issue, December.

Lloyd, I. J. (1997) *Information Technology Law* (London, Butterworths, 1997).

Loader, B., (ed) (1996) *The Governance of Cyberspace* (London, Routledge, London).

Lorek, L.A. (1997) "Outwitting Cybercrime" (Sun-Sentinel of South Florida) <http://www.sunsentinel.com/money/09130018.htm>.

Melossi, D., "Normal Crimes, elites and social control", in Nelken, D., (ed.), *The Futures of Criminology* (London, Sage, 1994), p. 205.

Post, D. (1995) "Encryption vs. The Alligator Clip: The Feds Worry That Encoded Messages Are Immune to Wiretaps" *New Jersey Law Journal*, 23 January.

Pretzlik, C. (1996) "Firm accused of fraud on the Internet" *Daily Telegraph*, 9 November.

Reiner, R. (1992a) *The Politics of the Police* (Hemel Hempstead, Harvester Wheatsheaf).

Reiner, R. (1992b) "Policing a Postmodern Society" 55 *Modern Law Review* 761.

Reno, Hon J (1996) "Law enforcement in cyberspace" address to the Commonwealth Club of California, San Francisco Hilton Hotel, 14 June, <http://pwp.usa.pipeline.com/~jya/addres.txt>.

Rheingold, H., (1994) *The Virtual Community: Homesteading the electronic frontier* (New York: Harper Perennial).

Rowland, D., and Macdonald, E. (1997) *Information Technology Law* (London, Cavendish, 1997).

Saradar, Z. and Ravetz, J.R., (eds.) (1996) *Cyberfutures: Culture and Politics on the Information Superhighway*. (London: Pluto Press) p. 1.

Seiber, U. (1998) "Legal Aspects of Computer Related Crime in the Information Society, Legal Advisory Board for the Information Market" <http://www2.echo.lu/legal/en/comcrime/sieber.html>.

Shearing, C. and Stenning, P. (eds.) (1987) *Private Policing* (Newbury Park, Sage).

Sheptycki, J. (1998a) "Policing, Postmodernism and Transnationalism" 38 *British Journal of Criminology*.

Sheptycki, J. (1998b) "Reflections on the Transnationalisation of Policing: the case of the RCMP and Serial Killers" 26 *International Journal of the Sociology of Law* p. 17.

Standage, T. (1996) "Web access in a tangle as censors have their say" 475 *Electronic Telegraph*, 10 September.

Sterling, B. (1994) *The Hacker Crackdown* (London, Penguin Books).

Sussman, V. (1995) "Policing Cyberspace" 38 *U.S. News*, 23 January, p 54.

Tendler, S. (1996) "Public to help police curb Internet porn" *The Times*, 2 December. Internet Watch can be found at <http://www.Internetwatch.org.uk/>.

Uhlig, R. (1996a) "Minister's warning over Internet porn" *Electronic Telegraph*, 16 August.

Uhlig, R. (1996b) "Hunt is on for Internet dealer in child porn" 518 *Electronic Telegraph*, 23 October.

Uhlig, R. (1996c) "'Safety Net' on Internet will catch child porn" 488 *Electronic Telegraph*, 23 September.

Walker, C. P. (1997) "Cyber-contempt: Fair trials and the Internet" 3 *Year Book of Media and Entertainment Law* (Oxford, Clarendon Press).

Walker, C., and Akdeniz, Y. (1998) "The governance of the Internet in Europe with special reference to illegal and harmful content" Criminal Law Review, Special Issue, December.

Wall, D.S. (1997) "Policing the Virtual Community: The Internet, cyber-crimes and the policing of cyberspace," in Francis, P., Davies, P., and Jupp, V., *Policing Futures* (London, Macmillan).

Wall, D.S. (1998b) 'Policing and the Regulation of Cyberspace', *Criminal Law Review*, December 1998, pp. 79-91.

Wall, D.S. (1999) "Cybercrimes: New wine, no bottles?", in Davies, P., Francis, P. and Jupp, V. (eds) *Hidden Crimes, Victimisation and Regulation* (London: MacMillan).

Wallace, J., and Mangan, M. (1996) *Sex, Laws and Cyberspace* (New York, Henry Holt).