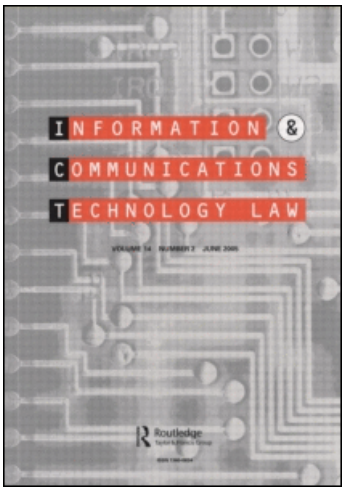

Information & Communications Technology Law
Publication details, including instructions for authors and subscription information:
http://www.informaworld.com/smpp/title~content=t713424803

I can see you: harassment and stalking on the Internet

Michael Salter [a]; Chris Bryden [b]
[a] Chambers of Ronald Thwaites QC, Ely Place Chambers, London [b] Chambers of Timothy Raggatt QC, London

Online Publication Date: 01 June 2009

To cite this Article Salter, Michael and Bryden, Chris(2009)'I can see you: harassment and stalking on the Internet',Information & Communications Technology Law,18:2,99 — 122
To link to this Article: DOI: 10.1080/13600830902812830
URL: http://dx.doi.org/10.1080/13600830902812830

Information & Communications Technology Law
Vol. 18, No. 2, June 2009, 99–122

Routledge
Taylor & Francis Group

I *can* see you: harassment and stalking on the Internet

Michael Salter[a] and Chris Bryden[b]*[1]

[a]*Chambers of Ronald Thwaites QC, Ely Place Chambers, 30 Ely Place, London, EC1N 6TD;* [b]*Chambers of Timothy Raggatt QC, Second Floor, 4 King's Bench Walk, Temple, London, EC4Y 7DL*

It is an inevitable consequence of plausible anonymity and deliberately lax regulation that the potential for 'virtual' harassment or 'cyber-'stalking, with the attendant possibility of threats, alarm, distress, slander and physical danger that go hand in hand with real world harassment, will increase the more widely available access to the Internet. The (relatively) recent explosion in casual exchange of personal information following the growth of sophisticated social networking platforms, the logical successors to more basic Internet chat-rooms, opens further the possibility of acquiring an unwanted connection with an obsessive party.

The authors consider the application of current UK legislative safeguards to the Internet, looking at the suitability of the Protection from Harassment Act 1997, data protection, unauthorised modification of computer software, libel law, external Internet regulation, Convention and Codes, and the potential for vicarious liability of employers where harassment is carried out by an employee, amongst other issues and conclude that there is a pressing need for primary legislation to counter the inadequacy and lacunae found in current domestic law. The authors go on to consider the extraterritorial application of such legislation and postulate the need for a re-balancing of the competing rights of freedom of speech and personal safety and wellbeing.

The authors further consider the potential liabilities of Internet Service Providers (ISPs), webhosts and Social Networking and chat-room forum sites, concluding that a shift in liability for Internet harassment from progenitor to facilitator is inevitable.

Keywords: Internet; harassment; stalking; cyber-stalking; reform; ISP; Protection from Harassment Act 1997

Introduction

It is an inevitable consequence of plausible anonymity and deliberately lax regulation that the potential for 'virtual' harassment, malicious comment or 'cyber-'stalking (collectively referred to herein as 'cyber harassment'), with the attendant possibility of threats, alarm, distress, slander and physical danger that go hand in hand with real world harassment, will increase the more widely available access to the Internet is. The (relatively) recent explosion in casual exchange of personal information following the growth of sophisticated social networking platforms, the logical

*Corresponding author. Email: cxb@4kbw.co.uk

ISSN 1360-0834 print/ISSN 1469-8404 online

DOI: 10.1080/13600830902812830
http://www.informaworld.com

successors to more basic Internet chat-rooms, further opens the possibility of acquiring an unwanted connection with an obsessive party.

Whilst there does exist a hodge-podge of legal remedies that can be applied to virtual harassment and cyber-stalking, there is little in the way of targeted protection for victims of such online behaviour, nor particularly effective sanctions, criminal or civil, for perpetrators. The most powerful shield available to an online user is probably the Protection from Harassment Act 1997 (PfHA 1997). However, an analysis of the scope and shortcomings of that Act demonstrates that whilst online harassment can be crow-barred within its exceptionally wide provisions, it is something of a blunt instrument, unwieldy and unsuited for a fast-moving online world. The requirement that the harassee shows a course of conduct amounting to harassment, with the acts forming that harassment equating to actionable criminal acts makes it difficult for someone suffering the posting of slanderous comments, or the taking over of email addresses, or the bombarding with messages, to obtain legal satisfaction, either by way of a prosecution or by the more usual civil claim for an injunction and/or damages. This is not to say that such claims can never be successful; as will be seen below there is an increased use of the Act in respect of Internet abuse. However, the Act is useful because it is so widely drawn; it is cumbersome and unwieldy and does not apply to all circumstances of cyber harassment.

The wider problem with existing legislation and other legal protection is that the remedies available are often not suited to the type of harassment experienced by online users. Damages or an injunction are useful where the perpetrator is known; so that, where a libellous comment is published by staff writers on a mainstream website, injunctive relief and a claim for damages or a swiftly printed correction provides a remedy. However, where a comment is posted anonymously on a message board, or where a sinister unknown is repeatedly sending messages from multiple untraced email addresses, a criminal prosecution or civil injunction cannot be targeted at the originator of such behaviour. It is in these circumstances that a harassee will often be advised to target the carrier of such unwanted activity, bringing a claim against the message board host[2] or against the email provider.[3] Whilst such action may be a temporary panacea it may be only a matter of minutes before the same activity recurs on a different message board or via a different email host or carried by an alternative ISP. Unless the root cause of the problem is tackled, injunctive or financial relief against hosts in the form of the existing available sanctions is not going to solve it.

That is not to say however that the solution to this problem will simply be a new legislative programme criminalising such behaviour. Knee-jerk legislation often does not fulfil the original purpose its draftsmen intended, and where dealing with the Internet the difficulties properly of framing preventative law are greatly magnified. Given the extra-territorial aspect of the Internet and the difficulty of applying domestic law to webhosts and Internet Service Providers based abroad, it is submitted that traditional domestic legislation, providing definitions of 'cybercrime', 'Internet stalking' and other such terms, will not assist in confronting such undesirable aspects of electronic interaction, and perversely would likely merely duplicate the existing legal framework criticised herein as inadequate.

Instead it is proposed that legislative intervention can more properly be directed at a new range of 'tools' or 'weapons' for law enforcement and for use by private individuals in the civil forum and which place a far greater emphasis on prevention by carriers, either by the mandatory production of information to assist a prosecution or a civil case, or by the placing of sanctions on identified individuals

for repeat offences, equivalent to the common perception of a 'restraining order', with serious penalties for breach. A further such weapon would involve sanctions against ISPs, message boards, email carriers and the like for knowingly or recklessly allowing or facilitating the breach of such a '*Internet abuse order*'.

Framework of UK legislative safeguards applicable to the Internet

The strength of English common law lies in its adaptability in the face of previously unconsidered behaviour. Since the advent of the World Wide Web in the early 1990s English law has adapted to the new challenges produced by this massive new forum. Internet connectivity in the UK has become the norm and communication over the Internet by way of email is ubiquitous. Instant messaging and forum posting are also commonplace. The challenges of this vast electronic system to law enforcement became clear in such fields as money scams (a simple development from old-fashioned postal scams), illegal pornography and other obscene materials (dealt with by direct legislation which applied equally to the Internet) and more recently terrorist activities.

Equally the challenges in respect of cyber harassment presented by the Internet have become more apparent in recent years following the explosion in use of the Internet following the so-called 'broadband revolution' which began in the UK around the turn of the century. A move from slower dial-up connections to 'always on' connectivity meant that the opportunity for acquiring an online harasser directly targeting an individual (as opposed, for example, to random sexual approaches in an Internet chat room) was greatly increased.[4] Similarly, the sheer size of the World Wide Web[5] makes the control of the flow of information (postings, emails, instant messages, articles) inherently difficult to police.

There has been little in the way of direct regulation of the Internet or the World Wide Web in English domestic law and it is only relatively recently that issues relating to online defamation and harassment have really come to the fore. This is, perhaps, surprising given the size of the Internet and the ability of anyone with even vague technical ability to create a website[6] but it may also represent a shift away from the informality of electronic communication as a medium and recognition by big business that their reputations can severely be damaged by defamation on the Internet. It may also be the case that, with the greater use of the Internet by the general population and the lessening of inhibitions when 'hidden' behind a profile, user name or email address, more opportunity for the gathering of personal details or the development of alarming attachments is provided.

Nonetheless it is clear, it is submitted, that whilst the current medley of statutory and common law provisions does provide some protection and recourse in certain circumstances, most particularly where the perpetrator is clearly identified, their ambit is limited in situations such as cyber harassment where it is not known who is targeting the victim. In such circumstances there is little that the law at present can do to assist. There is also evidence that the concept of cyber harassment is not always taken seriously, with advice to victims being simply to change their email address or to switch off their computers. Such advice ignores the serious effect that cyber harassment can have on victims, as well as the risk that such actions will embolden a perpetrator so as to cross from cyber harassment to physical harassment (McCall, 2003).[7]

Further even where a perpetrator is identified, there are lacunae in the legal framework which result from the lack of targeted legislation to combat such issues, and extra-territorial aspects raise further complications. The main relevant legal concepts, and their weaknesses in respect of cyber harassment, are considered below.

Protection from Harassment Act 1997

The Protection from Harassment Act 1997 (PfHA 1997) has, since coming into force on 16 June 1997, had its remit expanded significantly by the courts. It is now considered by some to be one of the most widely framed pieces of legislation enacted in recent years[8] and has been given a wide application beyond its original intention of dealing predominantly with the issue of stalking, following an empassioned campaign by Diane Lamplugh for legislation to protect people from others with an obsessive interest, following the disappearance of her daughter in 1986.

Whether the same was the direct intention of the legislation is open to question. However the same was clearly considered. When the PfHA 1997 was being debated by Parliament it was noted that:

> Stalkers do not stick to the activities on a list. Stalkers and other weirdoes who pursue women, cause racial harassment and annoy their neighbours have a wide range of activity which it is impossible to define.[9]

Previous attempts to pass an anti-stalking Act had failed. Those Bills contained a narrow list of activities that would be prohibited and would therefore trigger the operation of the sanctions contained within the Bill.[10] However, the PfHA 1997 did away with such a limited approach, and instead approached harassment in a non-exhaustive way. 'Harassment' is not a defined term within the PfHA 1997. Instead it states that harassment 'includes alarming a person or causing a person distress'.[11] This wide clause has ensured that many acts over and above stalking have been brought within its ambit and its application now covers a vast range of activity.

It is not enough, however, that an act falls within this broad approach to harassment. The conduct must occur on more than one occasion, or the victim must apprehend a second occurrence. This is because the PfHA 1997 requires a 'course of conduct'. This need not involve two acts directed at the same person. A harassor could, for example, on the first occasion send an abusive email to the victim and on the second post comments about a friend of the harassee on a Facebook page. Provided that it can be demonstrated that this conduct has a common motive, namely the harassment of the victim, then there nothing, is it is submitted, preventing these two acts being deemed a course of conduct.

The PfHA 1997 therefore does not require that there is a physical threat or a risk of immediate physical harm to amount to an actionable civil wrong. Further, the mixed criminal and civil aspects of the PfHA 1997 require only a fear of violence to commit an indictable offence. Similarly, conduct amounting to harassment will also amount to a criminal offence. In both the civil and the criminal aspects therefore, the PfHA 1997 is drawn far wider than laws introduced in various States of the USA with some States requiring a 'credible threat' of serious physical injury or death.[12] 'Credible threat' is defined for example in Wisconsin as 'a threat made with the intent and apparent ability to carry out the threat'.[13]

In answer to a Parliamentary question Maria Eagle (Parliamentary under-secretary, Ministry of Justice) stated that in 2006 a total of 5,446 prosecutions were

brought under PfHA 1997.[14] The summary offence is punishable by up to six months imprisonment whilst the either way offence carries with it a prison sentence of up to five years. Upon conviction, the court also has a power to impose upon the harassor a Restraining Order in an attempt to regulate the conduct complained of.

In addition to criminal offences (both summary and either way) the PfHA 1997, unlike other statutes aimed at curbing anti-social behaviour (such as the Family Law Act 1996), allows for the victim to seek compensation from the wrongdoer as well as injunctive relief prohibiting the wrongdoer from continuing with their conduct. Breach of any injunction is a criminal offence.

In this sense the wide drafting and even wider application of the PfHA 1997 is well suited to the challenges posed by the Internet. As the physical posting of a letter containing threats is clearly caught by the PfHA 1997, so would be the emailing of such threats. However, such inherent flexibility should not on an initial consideration of the application of the PfHA 1997 to the subject of cyber harassment be allowed to give rise to an unduly positive view as to its utility and effect. Where all parties are based within the jurisdiction it cannot be denied that the PfHA 1997 is of great assistance to cyber harassment, with criminal prosecutions and injunctions arising out of such cases.[15]

Recent press coverage has also demonstrated that claims are being brought successfully under the PfHA 1997, restraining online harassment.[16] Upon closer inspection however we respectfully suggest there are aspects of the legislation that may fundamentally weaken the utility of the PfHA 1997 in respect of its wider application, particularly in the field of cyber harassment. Whilst no-one can deny that the PfHA 1997 is a flexible and adaptable Act that has been applied in a number of distinct circumstances over and above its original intention (neighbour disputes and in the workplace to name but two), it may be this flexibility that is the 1997 Act's undoing.

Whilst the courts recognise the flexibility of the PfHA 1997, they at the same time have sought recently to rein in its effect, so as to ensure that it can be invoked only in the most serious incidents of harassment. For example, in the recent case of *Majrowski v. Guys & St Thomas NHS Trust*[17] the House of Lords made it clear that for the PfHA 1997 to apply the standard of conduct attributed to the alleged harasser needed to amount to criminal conduct:

> 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 that would sustain criminal liability under s2 [of the Act].[18]

This point was re-emphasised by the Court of Appeal more recently in the case of *Conn v. Sunderland City Council*.[19]

The requirement, in order to found a civil case against an alleged harasser, for the acts of harassment to amount to conduct which would found criminal liability presents an important hurdle to the suitability of the PfHA 1997 in respect of the Internet. The reason for this is that whilst many of the actions of the typical cyber stalker may be disturbing, unpleasant and may transgress the norms of socially acceptable conduct, they can rarely be said to amount to 'criminal conduct' when

judged against the case of *Conn*. In that case, a line manager confronted three members of staff (including Mr. Conn) to determine if they had left work early. When Mr. Conn failed to respond to his satisfaction the line manager shouted, and threatened to smash a window. On another occasion the line manager threatened to hit Mr. Conn. This behaviour was not categorised as amounting to harassment under the PfHA 1997 so as to allow the claim to succeed. Therefore, whilst sending emails that contain untruthful stories about a person via a social networking site to all of their acquaintances may be deeply unpleasant to the maligned person, it is arguable that such conduct does not break the law so as to amount to a criminal offence. Such conduct is of course libellous, but this may not be enough to invoke the protection of the PfHA 1997.

That is not, of course, to say that the PfHA 1997 is of no use in such circumstances. In extreme cases of cyber stalking, criminal boundaries may well be transgressed. However, the situation is not analogous to a person who repeatedly attends at the physical address of their victim, leaving cards, flowers, or even love letters containing oblique threats. Being in the same chat room is unlikely, in itself, to be enough to invoke the protection of the PfHA 1997, even if abuse has been targeted by that person at his victim before, whereas being in the same bar in similar circumstances might be. Whilst in both circumstances it may be a matter of degree, the latter situation is far more likely to result in a court treating the matter seriously than the former.

Further, the requirement that there be a course of conduct before harassment can be established may equally prevent the PfHA 1997 from applying. Does it amount to one act, or multiple acts to send one email, with one click of a mouse button, to a thousand recipients? From a straightforward reading of the PfHA 1997 it is submitted that the same would amount to a single act, even though the impact of that one action would be likely to be more alarming and distressing to a victim than two letters (or emails) being sent by the wrongdoer to separate people at separate times. This is, of course, an extreme example of the application of this provision of the PfHA 1997, but that illustrates the point in hand. The PfHA 1997 was not designed to combat issues of cyber stalking or other Internet related activities that result in a victim being frightened, alarmed, distressed, or any of the other buzzwords surrounding the legislation. Whilst it was enacted in the middle of the so-called on-line boom in the late 1990s, the PfHA 1997 was not designed to deal with cyber harassment.

A final, practical point in respect of the PfHA 1997 is that it applies only in England and Wales (a slightly amended version also applies in Scotland). Therefore, whilst it might be possible to require the police to bring criminal proceedings (which might depend whether the crime was committed in England and Wales or abroad) or to bring a damages claim, an injunction granted under the PfHA 1997 is likely only to restrain such conduct within the jurisdiction. The question must therefore arise as to whether any injunction obtained under a jurisdictionally limited Act has any effect at all where a harasser based abroad can simply continue their conduct unhindered. Whilst issues of extraterritoriality are considered in greater detail below, it is essential to make clear at this juncture that the value of injunctive relief of any sort is only of value with regard to the Internet if it can be enforced trans-nationally.

Whilst the PfHA 1997 does have certain strengths, and is clearly of benefit in the armoury of the watchman of the World Wide Web, it also has serious flaws when

considering the reality of the risk of cyber stalking. That it has weaknesses is, perforce, a result of its broad-based approach, rather than being legislation specifically targeted at the Internet. As discussed below, there is certainly some benefit in including injunctive relief as a potential remedy when reconsidering the legislative approach to cyber harassment, but the protection afforded from PfHA 1997 is so piecemeal, due to its broad-brush approach, that specific protections are required.

Vicarious liability for harassment by an employee

It is a well-known principle of the common law that in certain circumstances an employer can be held responsible for the wrongdoings of their employees by way of vicarious liability. The House of Lords has held this doctrine applies to claims brought under the Protection from Harassment Act 1997: *Majrowski v. Guy's and St. Thomas's NHS Trust*.[20] Mr. Majrowski, after an initial failure at first instance successfully brought an action against the NHS trust for harassment based on the conduct of fellow employees towards him.

The scope of vicarious liability has recently been greatly expanded from the longstanding defence allowing an employer to escape liability if the employee could be shown to be 'on a frolic of his own'. The House of Lords in *Lister v. Hesley Hall*[21] removed this defence and substituted a new test. For an employer now to be liable for the acts of a tortfeasor employee the act in question must be 'so closely connected' with the work the employee was employed to do that it is just and equitable to hold the employer responsible. The 'close connection' test has subsequently been refined and extended, but the emphasis is clear: the court will concentrate on the relative closeness of the connection between the nature of the employment and the particular tort and then ask, looking at the matter in the round, is it just and reasonable to hold the employers vicariously liable.[22] The close connection test has been applied widely and catches behaviour which would otherwise have escaped vicarious reference to the employer.[23]

An employee who harasses another, physically or via the Internet, may be doing so in circumstances where his employment merely gives him the opportunity to commit the tort (say by posting details about an ex-partner on their Facebook page). However, depending on the circumstances it may mean that harassing behaviour were acts done in the course of that employment (for example by posting defamatory comments in respect of a customer on a forum). In such circumstances it is possible that the employer will be liable for any tortious wrong committed, if it is fair and just for the court so to hold them liable. It is therefore feasible that a victim of cyber harassment could consider bringing a claim against an employer, where the relationship between the perpetrator and the victim was connected to the employment of the former.

In a reversal of this situation, the authors have previously set out their arguments for the proposal that pursuant to the PfHA 1997 a harassed victim may, in certain circumstances, be able to seek redress against their employer for harassment caused by third parties, provided that the employer is aware of the harassment taking place.[24] Therefore, if an employee notifies his line manager, or the IT department, that he is the subject of harassing emails from a customer of such a nature that cause him alarm or distress, it is possible that he would be able to succeed in a claim against his employer, provided he could get over the hurdle imposed by *Conn*.

The reality of modern working environments is that most jobs now require and provide computers and access to the Internet. The provision of such access will inevitably result in employers who find their errant employees stalking or harassing others, be they fellow employees, or third parties, being held liable for their actions. The liability of the employer will of course be strict.

This aspect of English domestic law is in effect an extension of the application of the principles set out in the PfHA 1997 and serves further to illustrate that whereas current legislation does provide some assistance (particularly where harassing behaviour, in the physical world or online, amounts to criminal conduct), it does not fully address the issues raised by cyber harassment.

Defamation

A powerful weapon available to a victim of malicious statements on the Internet is the law of defamation, loosely defined as 'the publication of a statement which tends to lower a person in the estimation of right-thinking members of society generally'.[25] Where the creator of a malicious website or creators of defamatory statements, emails or postings can be identified, it is usually fairly straightforward for a claim for compensation to be brought against that person, provided, of course, that they are of sufficient financial substance for this to be worthwhile. Together with such a claim, or as a standalone remedy, an application for an injunction requiring the removal of such information is likely to be an effective remedy.

Such claims can result in significant financial compensation as well as ruinous costs. Earlier this year an award in the region of £100,000 was made against John Finn, who had created anonymously a website known as 'Dads Place' which was the conduit for various seriously defamatory allegations on what was described as 'a seriously defamatory, abusive and scurrilous anonymous website'.[26] Other high profile UK cases include the Gina Ford action against the Mumsnet website and the action brought by advertising agency WPP against Fullsix Spa.[27]

However, it may also be possible to claim against the publisher of defamatory statements. Whilst there are a number of defences available to a Defendant to any defamation claim, including privilege, fair comment and most understandably, truth, it is clear that in many cases an ISP or other service provider will not be able to avail itself of these defences, as they rely upon information that is likely to be known by the actual person who creates the blog entry or posts the comment, but not the ISP itself. Indeed, the sheer scale of communication and posting online make it virtually impossible (if not totally impossible) for an ISP to police its own email/hosting or newsgroups.

Nonetheless, defences exist to actions for defamation against secondary publishers. In the 1990s during the initial stages of public access to the World Wide Web, the law began to develop firstly in the US (where a series of contradictory decisions turned on arguments relating to adoption of content and the like). In the United Kingdom the case of *Godfrey v. Demon Internet Ltd*,[28] defined the scope of the main defence provided to secondary publishers. The Defendant ISP sought to rely upon the defence contained in Section 1 of the Defamation Act 1996, which provides a defence if the secondary publisher took reasonable care in relation to the publication of the defamatory material, and did not know, and had no reason to believe, that what he did caused or contributed to the publication of the defamatory statement. Demon failed in its defence, as they had been told some 10 days earlier by

Mr. Godfrey that a posting purportedly from him and giving details of his email address was a forgery; coupled with a request to remove the item. Moreland J rejected the argument that Demon was within Section 1 and found that it was in a similar position to a bookshop or library: once it knew of the material it had decided how long to store it.

Godfrey was determined prior to the introduction of the further protections contained in the Electronic Commerce (EC Directive) Regulations 2002 came into force. Internet Service Providers and other service providers now benefit from protection from claims brought against them due to the provision of defences by the Electronic Commerce (EC Directives) Regulations 2002[29] ('the 2002 Regulations'), in addition to Section 1 of the Defamation Act 1996, in relation to information they have carried, hosted or cached but did not create. Therefore a victim of cyber harassment or malicious comment cannot simply bring a claim in compensation against the host.

The 2002 Regulations apply to 'information society services' which amount to any service normally provided for remuneration at a distance, by electronic means and at the individual request of a recipient of the services. Collins (2005) has noted that 'Commercial Internet intermediaries, such as ISPs, bulletin board operators, and web housing services will usually satisfy this definition'.[30] There is a degree of uncertainty as to whether therefore a University, for example, is covered by these regulations and so has the defences open available to them, as access is not provided for remuneration. In *Bunt v. Tilley*[31] Eady J noted that Gatley on Libel and Slander[32] stated that a fee-paying university may be covered by the Regulations as it provided this service for remuneration, even if there was no identifiable charge. The definition therefore is a wide one, and is likely to cover many of the obvious conduits (as opposed to hosts) of malicious or harassing statements or actions.

Regulation 17 provides a defence of acting as a mere 'conduit' and Regulation 18 deals with defences relating to the caching of certain information. Gatley (2003) notes that the protection is therefore aimed at transient messages, such as e-mail, or at more permanent material which simply passes through the systems of the service provider for the purposes of access, rather than material which is stored for significant periods. Knowledge on the part of the service provider is irrelevant, so no liability attaches for a failure to take steps to prevent access to another site which the provider is aware carries defamatory material. However, the Regulation does not confer immunity against the grant of an injunction.[33]

The 2002 Regulations therefore confer powerful protection on ISPs and other service providers in respect of compensatory claims where they have simply facilitated in the course of their business defamatory or malicious words or acts. However, this protection is not absolute and importantly does greatly alter the position in the *Godfrey* case. Therefore where an ISP knows or is aware of potentially defamatory material and still does nothing, liability may still ensue. As Eady J in *Bunt v. Tilley*[34] noted:

> 21. In determining responsibility for publication in the context of the law of defamation, it seems to me to be important to focus on what the person did, or failed to do, in the chain of communication. It is clear that the state of a defendant's knowledge can be an important factor. If a person knowingly permits another to communicate information which is defamatory, when there would be an opportunity to prevent the publication, there would seem to be no reason in principle why liability should not accrue. So too, if

> the true position were that the applicant had been (in the claimant's word) responsible for 'corporate sponsorship and approval of their illegal activities.
>
> 22. I have little doubt, however, that to impose legal responsibility upon anyone under the common law for the publication of words it is essential to demonstrate a degree of awareness or at least an assumption of general responsibility ...[35]

It is clear that a complicit service provider will therefore not be able to escape liability. However, the framework provided by the 2002 Regulations is a powerful protection. The proposals submitted by the authors of this paper for further regulation must therefore bear in mind this aspect of protective legislation, though it is the view of the authors in any event that injunctive, non-punitive remedies are the most favourable way to approach Internet regulation with regard to bodies other than the direct perpetrator of acts amounting to cyber harassment.

ISPs have complained to the Law Commission that they feel they are 'tactical targets' for those who wish to prevent dissemination of material via the Internet[36] with pressure brought to bear upon them to remove material without any real opportunity to consider the true nature of the alleged defamatory statements. The Law Commission Report notes the possible conflict between pressure to remove the material and the emphasis upon freedom of expression under the European Convention of Human Rights. The 2002 Report further noted that many organisations, in answer to consultation from the DTI, asked for clear-cut 'notice and takedown procedures' to be established with the Internet Service Providers Association recommending a code of practice underpinned by statute be set up to reduce the circumstances in which ISPs were held liable for defamatory publications by users of their services.

Self-regulation

Given the apparent inability of traditional legal remedies fully to regulate conduct amounting to cyber harassment, the focus of attempts to reduce such activities must turn to the providers of online services themselves: the ISPs, the networking sites, the email service providers. Whilst it is arguable that peer pressure to some extent regulates the conduct of other users online,[37] it does not follow that peer pressure can deter a determined stalker from harassing his victim. Whilst libellous posts or hurtful messages may be flagged by users and removed by moderators, this does not prevent the root of the problem – that a person determined to harass and victimise another person can do so, and can operate beneath the view of his peers, by private messaging, email, or on a webpage he sets up himself.

The difficulty posed by self-regulating codes of practice is that by their nature such codes are not mandatory. Such codes of practice are also necessarily interest-driven, with the framers ensuring that their respective positions, beliefs and ideals are central to their code. Whilst respectable sites may sign up to them, it will relatively rarely be such sites that allow such behaviour to take place, or, conversely, such sites are so large that they are unable actively to police themselves, rendering any code otiose. Further, even with codes of best practice, non-compliance is unlikely to lead to any meaningful sanction. At worst a website or provider is censured for non-compliance, but unless a code of practice is mandatory and failure to comply leads, for example, to a loss of a licence, it lacks the teeth to ensure that it is adhered to. It is clear that no such sanction could be imposed on the World Wide Web: it is simply too large.

That is not to say that voluntary codes of practice are of no use at all. On the contrary, users of sites that claim membership to a code may be reassured, and should any malicious or harassing behaviour be reported, it may be that members of such a code of practice are able to establish a clear method for dealing with such difficulties. Likewise, an agreed code allows users to know what is or is not acceptable and how to deal with problems, and conversely for hosts or content providers or creators to work within an agreed framework of acceptability. An example of such is the proposed draft code of conduct of Orielly (2007) for bloggers and blog sites.[38]

It is submitted however that a Government-led, fully consulted code of practice dealing with the issue of cyber harassment may, however, be able successfully to be introduced, provided that it sets out a minimum required standard, and is incorporated into a package of remedies. Our proposals are set out more fully below.

Current safeguards are inadequate to protect from virtual harassment or cyber stalking

It can be seen from this brief examination of the primary legislative and common law principles applicable to cyber stalking that, it is submitted, whilst protections are provided in certain situations, there will be a large number of occasions where the current protections do not apply. There will be issues of harassment where PfHA 1997 is not engaged; malicious comments that do not amount to libel and other aspects of behaviour that simply do not conform to the current structure of the law. Whilst it is possible that further evolution of the law, particularly in the field of harassment, might mean, in time, that the common law expands sufficiently to encompass the situation where a person in a chat room is consistently flamed, or multiple email addresses are bombarded to tirade a woman with abuse, or where false profiles of a man are constantly being created over various fora, it appears at present that such victims are unlikely currently to be able to seek recourse. Likewise the law of defamation will assist them only in certain circumstances, and probably only if they are rich, or reckless as to the consequences of launching a lawsuit.

That English law is insufficient to deal with the multitude of possible cyber sins is unsurprising. Whilst, as already noted, the greatest aspect of the common law is its adaptability to new circumstances, the Internet is immutable, constantly changing, and so vast that every page cannot be actively policed. As seen in the criminal field, effective enforcement of the law in the face of money laundering, paedophilia and terrorism so often relies upon sting operations or lucky catches of people taking their computers in to repair.[39] Likewise, the law as it currently stands is not able to deal with the aspects of the Internet that make it so appealing to cyber stalkers – in particular its anonymity.

The law has always struggled with dealing with anonymous wrongs. In the criminal sphere huge resources are given over to detection of crimes. However, dealing with the civil remedies, either by way of injunctive relief or damages, is far more complicated. The average victim of cyber harassment or Internet libel is not able to spend thousands of pounds investigating the identity of the perpetrator of the wrong. The said perpetrator may also be able to shield himself from detection by using an alias and attempting to shield his computer IP address, or by using an Internet cafe. In order to hope to trace such a person an individual pursuing a civil remedy requires further information that is unlikely to be forthcoming from a simple direct approach to an ISP.

In the circumstances it is submitted that the current protections afforded to victims of wrongs perpetrated via the medium of the Internet are insufficient. Whilst it may be possible to consider a claim for damages or an injunction pursuant to the PfHA 1997 or by way of a defamation claim, or to bring claims against an employer on a tortious basis, or to consider whether there is a cause of action under the Data Protection Act 1998 or any other method, no remedy afforded under any of these remedies will quickly and effectively provide protection from an onslaught of harassment over the Internet, particularly if it cannot be demonstrated that the harasser is based in England and Wales. It is therefore submitted that existing safeguards are inadequate to deal with such circumstances. The only realistic way forward is for new legislation, not to regulate the Internet or to provide a draconian code, but to ensure that such victimisation is not tolerated and is dealt with, with the severity it deserves.

Need for primary legislation

It is acknowledged that the introduction of directed primary legislation is likely to be fraught with difficulties. In particular, the anonymous nature of the Internet, coupled with its extraterritorial existence, will cause difficulties in identifying perpetrators and enforcing remedies against them where jurisdictional issues arise. However, it is submitted that there is sufficient inadequacy in the current legal framework to require intervention, particularly following the recent growth in Internet usage. Whilst the proposed remedies suggested herein are not an overarching panacea for all of the ills of the Internet, they go some way to combating the issues of cyber harassment and related harm, by way of the introduction of a new Internet Abuse Order, mandatory disclosure of information giving the identity of perpetrators, a best practice code for social networking and message-board sites and a new civil wrong and criminal offence of knowing assistance in behaviour likely to breach an Internet Abuse Order.

Such regulation runs counter to the presumed 'live and let live' ethos of the Internet, as examined in greater detail below and some commentators have advocated a relaxation of regulation in respect of the online community. In their recent paper, Basu and Jones (2007)[40] examine the issue of what they term 'cyberstalking'. Whilst the remit of their work follows a broadly parallel approach to that adopted herein,[41] the conclusion of that paper is confounding. They conclude:

> We cannot regulate cyberspace without an understanding of cyberspace. In the case of pure cyber stalking, the nature of the community, the activity and the actors lead us to the conclusion that rather than considering the form of the regulation we should considering [sic] whether there can be any regulation at all. Rather than accept inappropriate regulation we would urge that in relation to pure cyberstalking consideration be given to a regulatory free approach.

With respect to the authors of that paper, their conclusion, based on an examination of current regulation and its applicability to cyberspace and a concern that regulation 'may destroy the very form and nature of the behaviour and the environment will be left the poorer' overlooks the very real harm that can ensue from such behaviour. Such a conclusion rests on a false separation between physical and cyber stalking combined with a belief that 'a digital realist perspective would suggest that Internet users should tolerate some stalking as users choose to enter cyberspace

with knowledge of the nature of the community and pervasive anonymity', further compounded by a failure to appreciate to any great extent that regulation short of criminalisation (for example by way of injunctive relief) may be appropriate.

It is unclear whether the authors of that paper are calling for the wholesale disapplication of any form of regulation to the Internet, so legitimising cyberstalking. This certainly appears to be the inexorable logical progression from their conclusion. However, it is submitted, to distinguish between predatory and malicious behaviour that takes place in the physical and the cyber world, is misguided and dangerous. The three differences highlighted by Basu and Jones (2007) do not stand up to scrutiny. They argue that the nature and form of online behaviour leads to differences, such as lack of confrontation, and give the example of a potential stalker sending harassing electronic communications to a victim, rather than confronting them in person or by telephone. It is submitted that this is no difference at all: a 'real world' stalker may simply send threatening letters or write intimidating notes. They argue that 'a significant number of cyberstalking victims do not know the identity of their harassers', giving a qualitative difference between offline and online stalking. But it is a generalisation to state that physical stalking victims will usually know the perpetrator, and in any event such anonymity makes regulation all the more important. Finally, a distinction is drawn between the nature of the acts that constitute stalking. However, it is submitted, whatever medium is used to act in a way that causes harassment, alarm or distress, it is the effect of such behaviour that is the constituent of stalking or harassment. That Basu and Jones (2007) fall into error when categorising cyberstalking separately to 'physical world' stalking is illustrated by the quote they themselves utilise:

> to argue that an act of cyberstalking is less serious than stalking will grant a would-be offender the right to harass, humiliate or defame individuals simply on the basis that it is not 'real'. There is always attempt made by some commentators to oversimplify what is a far more complex act of crime for 'the sake of a presumed theoretical, methodological or philosophical bias.[42]

It is submitted, on the contrary, that cyber harassment is simply another aspect of an offence, that which is loosely defined in PfHA 1997 (by inclusion) as being an act likely to cause alarm or distress. That the medium over which such behaviour is conducted or communicated is electronic does not change its character or make it any more excusable. That the Internet may provide greater opportunity for such behaviour does not make it acceptable. That the tool of cyber harassers causes difficulty in tracking down and controlling offenders does not mean that regulation should be avoided. And just because acts committed on the Internet may fall short of criminal behaviour does not mean that they should simply be ignored. Rather, further regulation is required in order to ensure that victims of such behaviour can take steps to halt it, to hold perpetrators to account financially, and if necessary, effect sanctions against hosts or carriers of such acts as a last resort.

Anonymity

It is accepted that, when considering the elements of cyber harassment, the anonymity of the perpetrator will often be more pronounced than in many physical-world stalking cases. Anonymity is a fundamental aspect that underlies much Internet communication, and the fluidity of identity is said to be one of the chief

attractions of this method of social intercourse.[43] The use of online pseudonyms, tags, aliases and character names, be it on social networking sites, by virtual communication using instant messaging or the conversations in computer games, is a widespread and accepted part of such interaction. Anyone can strike up a conversation online with another simply on the basis of a chance meeting, perhaps on grounds of a common interest or from a networking site or social group. However, the identity of that person, and the quality of the information imparted, is likely to be taken at face value, albeit with perhaps some degree of cynicism by the other party. Nonetheless the huge growth in Internet communication of all forms is testament to the willingness of people to interact socially at all levels despite, or perhaps because of, the cloak of anonymity and the shield of privacy that it provides.

For the majority of its users anonymity and pseudonimity (the use of a fictitious name) are empowering tools. Users can discuss topics they may feel constrained about discussing directly with another person face to face. Indeed, various organisations use or have used programs designed to anonymise the emails they receive, such as police forces, Amnesty International and the Samaritans. Specialist organisations such as the Internet Watch Foundation (IWF) and the Child Exploitation and Online Protection Centre (CEOP) rely for tip-offs on the anonymity granted to those reporting matters of concern. Clearly anonymity in and of itself is not a negative aspect of the Internet – quite the opposite in that it promotes freedom and breaks down inhibitions. Anonymity is an accepted and respected feature of online interaction, which forms part and parcel of that interaction. Even if it were considered necessary to bring to an end the anonymous nature of the Internet in the interest of preventing cyber harassment, the same would prove entirely impossible.

However, the plausible anonymity inherent in all Internet communications, the use of software to disguise the origin of emails as well as the simple provision of false information all may allow a determined perpetrator to disguise his identity should he so wish. Equally, in signing up for an email account with a provider such as hotmail.com, whilst details are requested of name, date of birth, address etc, it is entirely possible to enter false details so as to disguise a true identity.

That said, ISPs in England and Wales do not provide anonymous accounts. It should therefore be possible to obtain details in respect of details of a cyber stalker by enquiring of the ISP. ISPs assign an Internet Protocol ('IP') address to individual computers and other connective devices, and it is possible in most cases to ascertain the location of the physical computer assigned to that address. Equally, instant messaging providers such as Microsoft Instant Messenger or AOL, and email providers will often be able to trace physical addresses of users (Orlowski, 2004).[44] Clearly, however, an ISP is unlikely simply to provide information to a victim at their request. Rather, legal proceedings are required, and at present may pose difficulties outwith the criminal sphere.

There have been a number of cases in America where, following alleged defamatory, malicious or harassing comments, a lawsuit is launched so as to allow a sub poena to a web site or ISP to obtain the identity of the poster. Such cases have been dubbed 'cyberslapps'[45] (Strategic Lawsuits Against Public Participation) and have invoked a backlash by campaigners seeking to maintain anonymity.

It should also be noted that the current jurisprudence in respect of issues relating to privacy is developing at a fast pace. Cases such as the recent *Mosley v. News Group*

Newspapers Ltd[46] illustrate an area that is growing in significance. Anonymity and pseudonimity confer a certain degree of privacy, and it may be that there is scope for challenges based on the 'right' to privacy as a defence to attempts to obtain details of harassers held by websites and ISPs.

The website WHO@ (Working to Halt Online Abuse)[47] compiles statistics of online harassment based on detailed questionnaires sent out to those who report such actions to them. The site states that it deals with an estimated 50–75 cases per week and its statistics are based only on those who fully complete questionnaires. The comparison statistics for the years 2000–2007 are enlightening. Or a total of 2,256 respondents, 49% of perpetrators had a relationship to the victim, of whom the largest majority (34%) were ex-partners, followed by online acquaintances (17.25%). 36% of respondents reported that the harassment began via email. Whilst these statistics represent only a small sample, they do demonstrate that a significant number of reported incidences of cyber harassment is carried out by an identifiable person.[48]

The topic of Internet privacy falls outside the ambit of this paper, and has exhaustively been discussed elsewhere (Wafa, 2008).[49] Nonetheless it appears tolerably clear that unless fairly advanced steps are taken to disguise identity, it is possible for ISPs and other service providers to obtain information, including physical location, of users of the Internet.[50] Similarly, even the use of anonymisers or anonymous emails runs the risk of tracing.[51] A case in point is that of Bruce Hyman, a barrister convicted in 2007 of perverting the course of justice. In the course of representing a mother in a case involving contact and residence of her child, Mr. Hyman attempted to incriminate the father by sending him false legal documents via email, under cover of the faked logo of the pressure group Families Need Fathers. The father presented the case to the Judge, believing it to be genuine, and Mr. Hyman then alleged an attempt to mislead the court. However, the father was able to trace the email to an Internet café, where CCTV footage enabled him to identify Mr. Hyman.[52]

Nevertheless, a real difficulty in formulating methods to protect against cyber harassment is the ability of determined cyber harassers potentially to hide their identities. There is no cure-all for this real difficulty, as a determined perpetrator will be able to hide behind a multitude of aliases, IP addresses and email addresses. Therefore the approach to regulation must be three-fold: to minimise the possibility of successfully hiding, and therefore providing a deterrent; to provide the tools to track down perpetrators as far as is possible by the mandatory provision of information; and to provide effective sanctions where cyber harassment is shown to have taken place, or to have been allowed, intentionally or recklessly, to continue.

Balancing freedom of speech against personal safety and well-being

That the Internet prides itself as a champion of freedom of speech is well-established.[53] Whilst it is possible to censor or block access to sites, either by control of ISPs with threats of sanctions or by countrywide firewalls,[54] the ethos of the Internet is to allow (anonymous) free speech, and there are a multitude of campaigns to protect this 'right'. There is clearly therefore a tension between regulating the content of the World Wide Web to protect against malicious or harassing behaviour, and what is seen as an absolute right of freedom to post anything online.

This is recognised by the courts. In *ACLU v. Reno* Judge Dalzell stated that:

> ... as the most participatory form of mass speech yet developed, the Internet deserves the highest protection from government intrusion. Just as the strength of the Internet is chaos, so the strength of our liberty depends upon the chaos and cacophony of ... unfettered speech.[55]

The right to freedom of expression is protected by the European Convention of Human Rights Article 10, though this right is not absolute. The tension between freedom of expression and protection of the individual from harm, be it physical, threatening or defamatory, is longstanding and variable in accordance with prevailing political and social norms. Nonetheless, it is a tension that must be recognised to allow a balance to be struck when considering the effect of proposed legislation to regulate such behaviour.

The authors consider that in balancing these two important competing rights, it is essential that sufficient weight is given to the potential for harm, emotional or physical, that cyber harassment may entail. In weighing the right of an anonymous individual to wilfully do acts that have the effect of causing harassment, alarm or distress against the right of any person not to be exposed to such acts, it is submitted that the scales must be tipped against freedom of expression in favour of protecting the individual. This is not to minimise or ignore the importance of the right to freedom of expression, nor to ride roughshod over established Internet principles. However, such principles are not absolute (Millar, Nichol, & Sharland, 2009)[56] and when held against the right of an individual not to suffer harassment, the latter must prevail.

Extra-territorial issues

The growth of the Internet, and of access to it, show no sign of abating. More and more computers in an ever growing community demonstrates a real challenge that faces any attempt to regulate the conduct of those who have access to a modem and a PC across the world.

The global nature of the Internet, and more particularly, the servers that host the World Wide Web, means that issues of jurisdiction will often be an issue in targeting the perpetrators of online acts of harassment or stalking. It is accepted that these issues will not be resolved simply by the enactment of fresh legislation as proposed in this paper, though it may go some way towards alleviating the problem. However, a truly global approach to the issue of Internet harassment may require each jurisdiction to enact and police its own legislation, or to sign up to reciprocal enforcement arrangements. Many countries have addressed the issue of harassment by way of legislation, though as in the UK this is often ill-suited to some of the issues relating to cyber harassment. The appeal of domestic legislation is that countries can take steps to ensure they can target what they see as the risks that their populations face, with the laws generally reflecting the values, religion, or principles of the relative jurisdictions. However, differences in cultural opinion may mean that a person is committing no offence in their own country but is committing an offence in the country of the person towards whom his behaviour is targeted. There may be no symmetry between the different jurisdictions, and any agreement as to an international definition of Internet harassment is unrealistic.

In any event, an approach involving international co-operation, whilst appealing on a simplistic level, is unlikely effectively to regulate and prevent Internet harassment. In addition, as with all attempts to fit square pegs into round holes, the difficulties in applying the different parts of current domestic legislation imposing civil liability is likely to be doomed to failure once the multinational reach of the Internet is weighed in the balance. For instance, what is the result where conduct complained of would trigger the application of the PfHA 1997 in England and Wales but not in Peru where the victim is based? Further complications arise where the networking site on which the victim is being harassed is based in a third country.

The principles arising from the area of conflict of laws may provide an answer in some cases. However, actions with an international element can be highly expensive and to pursue a claim may, in all reality, be disproportionate to the effect, particularly if the only practical enforceable remedy is pecuniary compensation.

Since the enactment of the Private International Law (Miscellaneous Provisions) Act 1995 the general rule is that is that the applicable law is the law of the country in which the events constituting the tort in question occur. Section 11(2) then adds qualifications to this principle with regards personal injury and damage to property. However, the entirety of Section 11 can be displaced when it would appear that to be more substantially more appropriate of the governing law to be that of another country altogether.

The effect of other legislation also demonstrates the inherent limit that national sovereignty imposes with regard to creating criminal sanctions for cyber harassment. For example, the Telecommunications Act 1984, whilst addressing international communications, and making it an offence *within* the UK to send offensive material over a telecommunications system (Section 42), expressly provides that it is not an offence to send the same material INTO the UK from abroad. Further, successfully bringing a prosecution against a cyber harasser may prove to be impossible if the conduct of that person is not criminal in their country. Moreover, even where criminality is demonstrated the issue of extradition would need to be considered.

In formulating protective legislative remedies, therefore, it is important to focus on the need to be as effective as possible within the jurisdiction. In allowing the courts to hold service providers responsible for the enforcement, where necessary, of Internet Abuse Orders, backed up by financial sanction for non-compliance, some jurisdictional issues can be avoided. Nevertheless it must be recognised that a complexity of Internet regulation will be the requirement at times to attempt to enforce orders abroad. A discussion of reciprocal arrangements is not within the scope of this paper but is a topic that the authors intend to return to at a later stage.

A proposed way forward

The forgoing examination of the existing framework of legislation and common law principles makes clear that consideration of further regulation of the Internet to provide some protection against cyber harassment must take into account issues relating to the inherent anonymity of Internet usage and the issues relating to extra-territorial application, whilst remaining sympathetic to the countervailing principle of free speech upon which the Internet is founded. Nonetheless, it is submitted that there is a need to introduce specific remedies aimed at protecting victims of cyber harassment to supplement the inadequate current framework and to deal with issues of anonymity and extraterritoriality. The authors have come to the conclusion that,

in order to safeguard the wellbeing of Internet users subjected to cyber harassment, such remedies must target both individual wrongdoers and service providers, who must shoulder a greater burden of self-regulation.

Our first proposal is the creation of a new type of Order, which we have dubbed an Internet Abuse Order ('IAO'). The purpose of an IAO is to allow the courts to regulate conduct where harassing, alarming or other behaviour is demonstrated. The framework of the IAO is modelled on the extant Non Molestation Order ('NMO'), which a County Court can grant in certain circumstances pursuant to the Family Law Act 1996 (as amended),[57] but goes considerably further in scope and application.

It is proposed that an IAO should be able to be granted by a County Court on an initial ex parte basis so long as prima facie proof of conduct likely to cause harassment, alarm or distress to the complainant, or actions objectively likely to cause damage to his reputation is produced. In a procedurally similar way to an application for an NMO, a Respondent to the application will be entitled to refute the allegations, but on the basis that the onus to make such an application falls to him. In other words, once an ex parte order is served, it will continue in force unless and until the Respondent makes an application for its discharge, following which a hearing should take place to determine whether the order should continue. Further, borrowing elements of the PfHA 1997 and of the NMO, breach of an order would be both a criminal offence and an actionable civil wrong, with the further option open to the court to regulate the use of the Internet by a Respondent guilty of non-compliance, in the same way a Sexual Offences Prevention Order allows a criminal court to do.

It is envisaged that the definition of cyber harassment should be left deliberately vague, in line with the precedent set by the PfHA 1997, though in order to maintain a balance between remedying cyber harassment and protecting freedom of expression, the actions complained of must be significant, and more than, for example, harmless pestering. This compares favourably with the attempts of some US States to formulate anti-cyber stalking legislation. For example, California defines 'harassment' as:

> ... a knowing and willful [sic] course of conduct directed at a specific person which seriously alarms, annoys, torments, or terrorizes the person, and which serves no legitimate purpose. The course of conduct must be such as would cause a reasonable person to suffer substantial emotional distress, and must actually cause substantial emotional distress to the person.[58]

Florida approaches the issue by defining the term 'cyberstalk' to mean 'communication by means of electronic mail or electronic communication which causes substantial emotional distress & does not serve legitimate purpose'.[59]

The effectiveness of such an order in this form clearly requires the identification of the perpetrator for it to be of use. In many cases this will not prove to be a problem, where the harassing behaviour is carried out by an identifiable person. In such circumstances it is quite possible that existing remedies may assist the victim of such behaviour, by way of a claim for defamation or under PfHA 1997. However where such remedies are not available, the IAO will fill this gap.

In order to deal with cases of pseudonimity it is proposed that the court, when granting an IAO, should be able to exercise ancillary powers of disclosure against third parties such as ISPs, social networking sites and email providers so as to allow

an applicant to discover the identity, if the same is not known, of the perpetrator. Such a power is justified, it is submitted, as a matter of policy, on the basis that the right of the individual not to be harassed or defamed outweighs the right of the perpetrator to remain anonymous. Such powers would clearly also require a waiver of the data protection obligations of the information holder. The requirement that information is disclosed should also result in a shift towards more and better records being held, because it is proposed, as seen below, failure to prevent cases of harassment in the face of determined anonymity will ultimately found liability on the ISP.

Importantly, the making of an IAO against a known individual must also give rise to registration requirements for it to be effective. A central database containing details of ISP, IP address, email accounts and other identifying information would be maintained, with a requirement that the individual keep it up-to-date. The purpose of such a database is to keep a record of the Internet use of that individual. Should it be discovered that undisclosed accounts are opened which are subsequently used to breach the IAO by further acts of harassment against the same victim, severe criminal sanctions, coupled with the power to make an Internet Banning Order, would apply. This powerful deterrent would, it is posited, go some way to ensuring that an offender, once caught, would not offend again. Whilst such a mechanism will not deter the most determined of offenders, it is suggested that where sanctions are severe enough, offender rates will reduce (Knaggs, Serle, & Simonsen, 2003).[60]

More severely, where an IAO is in force, it is proposed that a new inchoate offence of knowingly or recklessly assisting in a breach be applied to service providers and other such organisations. For such a scheme to succeed, the central database of IAOs would have to be made available to all ISPs and service providers, whose responsibility it would be to take reasonable steps to ensure that they are not assisting in a breach. It is recognised that this is a significant burden to place upon service providers, who may be dealing with vast networks and millions of pages of information. However the responsibility would be to take reasonable steps to ensure that, for example, a person subject to an IAO is not granted a new, unregistered, email address, or does not visit message boards or social sites to which his access has been restricted.

Despite the difficulties expressed above with respect to the implementation of voluntary codes of practice, it is proposed that hand in hand with the enactment of legislation empowering the courts to grant IAOs a statutory code should be enacted following full consultation with ISPs and other service providers. The purpose of such a code would be to set minimum standards for complaint procedures, and also to encourage the retention of data which, subject to a court order requiring its production, should assist in identifying offenders.

The Code of Conduct would therefore target two main issues. Firstly, it is to be hoped that anonymity issues could largely be overcome by an increased requirement for personal registration. Data protection issues can be avoided by ensuring that such information is not necessarily held on a central database – it is enough that the information is accessible and any perpetrator traceable; that ISPs can already, in the main, identify most anonymous users should mean that compliance would not be too onerous, and would also allay the fears of some privacy campaigners. Secondly, by providing a minimum standard of complaint procedure, regulated by statute, such organisations would be required to operate within defined boundaries where issues were raised of harassing behaviour, defamatory comments and the like. It is

proposed that, by giving written (electronic) notice to a host, an individual would be granted the right to require the service provider to remove postings, deny access and otherwise take steps to minimise cyber harassing behaviour within a certain period of time (say seven days – a short period of time to minimise the harm suffered by the victim). Failure to do so without reasonable excuse would be an actionable wrong, sounding in compensation, but the onus would be on the person giving notice to show that the matter complained of caused harassment, alarm, distress or loss of reputation.

A service provider would also be provided with a defence to a claim for knowingly or recklessly assisting in a breach of an IAO if on receipt of notice, took steps to remedy this within the set time period. Such proposals run hand in hand with the IAO regime, but have the benefit of requiring a service provider to take action even where an IAO has not been obtained, due to anonymity or jurisdictional issues. Extraterritoriality will, of course, remain an issue, but with industry co-operation, it would be possible to extend the reach of such a scheme by requiring compliance not just by the secondary publisher but by the carrier. Where a perpetrator is not within the jurisdiction, so as to allow an IAO to have effect, the onus remains on the service provider to terminate the access of the perpetrator, though reciprocal agreements with other jurisdictions could allow enforcement of an IAO abroad.

Such a 'notice and takedown' procedure is not new, having been raised by service providers themselves in response to the consultation reported in the 2002 Law Commission report. Importantly, such a scheme would also not infringe the 2002 Regulations (save, perhaps, for pure conduits such as ISPs), as by its very essence the scheme would involve the giving of notice to the service provider.

There is a clear benefit to service providers, as well as to individuals, of such a scheme, as it is likely to reduce the circumstances in which an operator could be held liable by way of defamation or for harassment. However, such a Code would require sanctions for non-compliance, which would practically have to be financial in nature – it is not proposed that a licensing scheme is workable or practicable.

Against the argument that such regulation will simply drive persistent cyber harassers to take ever more ingenious steps to hide their identities, it should be noted that it will be in the interests of the service providers to ensure so far as possible that perpetrators can be identified. Where a malicious user repeatedly posts defamatory comments, or opens multiple email addresses to harass his victim, multiple notices will be served on the service providers. The cost of compliance will potentially be significant, so service providers will wish to identify as quickly as possible the identity of such a perpetrator, to allow the victim to obtain an IAO, thus shifting the burden of enforcement onto the victim, whilst providing a deterrent to the perpetrator due to the serious sanctions for breach of an IAO.

Whilst these proposals appear radical, requiring as they do wholesale legislation and a greater regulation of service providers and the Internet as a whole than most other liberal Western regimes, the authors submit that the time has come to ensure that the Internet cannot be used as a wilful tool for harassment and defamation. Whilst principles of anonymity and freedom of expression are important, there is a need for a specific and directed mechanism to control the actions of malicious individuals to ensure that they are not abusing the privilege of Internet access. Likewise, there is a need, identified by service providers themselves, for a method of determining where they have a duty to act on cyber harassment or defamatory comments.

Nevertheless the proposals we advocate and in particular the IAO, are vulnerable to the charge that they are draconian, introducing as they do serious sanctions and control mechanisms. The IAO would join a growing stable of what have been termed Civil Preventative Orders ('CPOs'),[61] such as the Control Order introduced to deal with terrorism, or the Anti-Social Behaviour Order (ASBO) introduced to deal on a micro level with behaviour that did not directly contravene criminal legislation but constituted a local irritation, ranging from loud music to insulting behaviour.

There has been a significant increase in the range and scope of CPOs in recent years. Alongside this has grown up a comparative weight of legal opinion, including criticism of the use of CPOs as a panacea to the ills of society, a full discussion of which is outwith the scope of this paper. However, much of the harshest criticism founds on the breadth of application of CPOs, both in terms of conduct that they can be used to prevent and the scope of the prohibition that the CPO imposes. Thus an ASBO can be used to prohibit a wide range of anti- social behaviour following only relatively minor behaviour. Ramsey characterises shared features of the many types of CPO as follows:[62]

- they are granted in civil proceedings, or administratively with some judicial supervision;
- they are granted on satisfaction of broad and vaguely defined conduct;
- their terms may be any prohibition (or mandatory term in some cases) deemed necessary to prevent future instances of the broad and vaguely defined conduct on which they are grounded; and
- breach of any of their terms is a criminal offence of strict liability

We gratefully adopt this characterisation. It appears clear that the proposed IAO would fall within the description of a CPO.

Ramsey also identifies a number of critiques of the CPO, the 'most systematic to date' being that by Simester and von Hirsch.[63] However, the basis of Ramsey's thesis is that despite the strident and severe criticisms levelled at CPOs, it is possible to reconstruct the 'claim to legitimacy' of the CPO (in Ramsey's case, the ASBO) based upon the normative proposition of the theory of vulnerable autonomy. On that basis, Ramsey goes some way to answer the several pertinent criticisms of the CPO, which he recognises as valid. In effect, he responds to valid arguments that the CPO criminalises conduct that is not wrong; does not require an element of culpability (in the sense of a cognitive mens rea); that the punishment is disproportionate to the seriousness of the conduct; that the vagueness and imprecision of the grounds for liability do not give fair warning of what may render a person liable to a CPO; and, fundamentally, that by imposing a CPO, a court rather than Parliament is laying down criminal prohibitions by contending that whilst these criticisms are legitimate (which, to a greater or lesser extent, they are), one of the reasons that the CPO 'enjoys its practical political legitimacy in the present may be that it institutionalises the protection of vulnerable autonomy'.

It is submitted that the IAO can properly be characterised as a CPO, and that, whilst the criticisms that attach to CPOs generally can equally be levelled against the IAO, the Ramsey approach to CPOs as filling an important role provides justification. The need for the IAO to protect and preserve individual autonomy outweighs the criticisms which can be levelled against it.

Conclusion

It is submitted that unless legislation as suggested herein is enacted, the worst of both worlds is likely to occur, with an increase in victims of cyber harassment coupled with a continued shift of liability to providers of services online, resulting in increased costs but no deterrence in respect of such behaviour. Case law suggests that this is happening already. The remedies available to victims of electronic harassment will remain the ill-fitting and undirected solutions provided by the current legal framework. Victims are likely therefore to continue to target the uninvolved carriers with claims for financial compensation, resulting in greater pressure on message boards, ISPs, email providers and webhosts to actively censor content based on their subjective (though potentially legally advised) appraisal of what should and should not be allowed to be said, or to shoulder the risk of litigation, passing on the costs to end users.

Whilst the current use of reporting schemes and moderators is to be applauded, the proposals for new legislation shift a much greater positive burden for regulating onto the service providers by way of information gathering and provision, and by ensuring that registered IAO subjects have limited access to their services, whilst requiring them to identify offenders, to minimise litigation costs to themselves. Further, in allowing individuals to be targeted, and their identities to be disclosed, the actual perpetrators of cyber harassment can be required to pay compensation or can be monitored and deterred from offending behaviour, helping to restate a social behavioural Internet norm.

Without the introduction of further remedies such as those set out within this paper, the Internet will continue to operate as a self-regulated open forum, with freedom of expression an inviolable principle despite the cost to victims of malicious cyber harassment. An inevitable consequence is therefore likely to be a development of the current legal framework, unfit as it is. This is almost certain to shift liability for financial compensation onto service providers. Whilst this could be said to be desirable inasmuch as it mirrors the current English jurisprudential shift of liability from individuals to (insured) companies, the targeting of carriers rather than the individuals responsible for such behaviour will, perversely, result in a norm of acceptability for those acts. The purpose of remedies directed at behaviour is not, primarily, to provide pecuniary compensation, but to deter and discourage it. Failure to do so results only in an increase in such behaviour, making the Internet a dangerous place for victims of harassment and stalking, both online and in the crossover to the physical world.

Notes

1. The authors are both practising barristers, Chris Bryden at the Chambers of Timothy Raggatt QC, 4 King's Bench Walk: http://www.4kbw.co.uk, and Michael Salter at Ely Place: http://www.elyplace.com. Any and all errors of fact or law are their own. Special thanks should be extended to Thomas Bailey, then a pupil, now a tenant at 4 King's Bench Walk for his assistance in researching this paper.
2. For example, the defamation claim brought by Gina Ford against Mumsnet: Sherriff, L, (11 May 2007). *Mumsnet settles with Gina Ford over defamation claims*. Retrieved September 2008, from http://www.theregister.co.uk/2007/05/11/ford_mumsnet/
3. Though it must be noted that there are some difficulties in bringing such claims, considered in further detail below.

4. Eazel, W. (28 February 2006). *Online stalking on the increase*. Retrieved September 2008, from http://www.scmagazineuk.com/Online-stalking-on-the-increase/article/33024/
5. According to Worldwidewebsize.com there were 27.77 billion indexed pages as at 29 September 2008 and one trillion URLs. See the official Google Blog at http://googleblog.blogspot.com/2008/07/we-knew-web-was-big.html
6. See, for example, www.michaelsalter.net
7. Cyberstalking: A New Challenge for Law Enforcement and Industry, cited in McCall, R, (5 October 2003) *Online harassment and cyberstalking: Victim access to crisis, referral and support services in Canada concepts and recommendations, victim assistance online resources*. Retrieved September 2008, from http://www.vaonline.org/
8. See, for example, Harris, J. (2000). *The Protection from Harassment Act 1997 – An evaluation of its use and effectiveness*. Retrieved September 2008, from http://www.homeoffice.gov.uk/rds/pdfs/r130.pdf
9. Mr David Maclean MP, Hansard, HC, 17 December 1996, Col 827.
10. Attempts at exhaustive definitions having briefly been popular: cf the Schedule attached to the Obscenity Bill 1999.
11. Section 7(2).
12. Ellison, L., & Akdeniz, Y. (1998). Cyber-stalking: the Regulation of Harassment on the Internet. *Criminal Law Review* (December Special Edition). *Crime, Criminal Justice and the Internet*, 29–48.
13. See http://www.danenet.org/dcccrsa/saissues/stalking.html
14. Maria Eagle MP, Hansard, HC, 30 June 2008, Col 685W.
15. E.g. *R v. Debnath* [2005] EWCA Crim 3472.
16. E.g. http://news.bbc.co.uk/1/hi/england/west_midlands/7033591.stm
17. [2006] UKHL 34; [2006] ICR 1199 HL.
18. Per Lord Nicholls, at 30.
19. [2007] EWCA Civ 1492, [2007] 2 All ER (D) 99.
20. Ibid.
21. [2001] UKHL 22; [2002] 1 AC 215.
22. Per Lord Steyn in *Bernard v. Attorney General of Jamaica* [2004] UKPC 47 at 18.
23. As in *Lister* itself, where the employer was held liable for the sexual abuse by the school caretaker of boys, as his employment and therefore his access to them, was so closely connected with his employment.
24. Bryden, C., & Salter, M. (2007). Third Party Harassment. *New Law Journal, 157*(7280), 960.
25. Halberstam, S. (2008). *Defamation and the Internet*. Retrieved September 2008, from http://www.weblaw.co.uk/articles/demon_defamation_and_the_internet/
26. See *Housing chief's record net payout*. Retrieved September 2008, from http://news.bbc.co.uk/go/pr/fr/-/1/hi/england/wear/7328488.stm
27. Werdinger, J. (29 March 2007). *Libel lawsuit by WPP Chief is settled for $235,000*. Retrieved September 2008, from http://www.nytimes.com/2007/03/29/business/worldbusiness/29libel.html
28. [1999] 4 All ER 342.
29. Statutory Instrument 2002 No. 2013.
30. Collins, M. (2005). *The law of defamation and the Internet* (2nd ed.). Oxford: Oxford University Press, at 17.03.
31. [2007] 1 WLR 1243.
32. Milmo P., Rogers W.V.H., Parkes R., Walker G., & Busuttil C. (2003). *Gatley on libel and slander*. London: Sweet & Maxwell.
33. Paragraph 6.26, cited in *Bunt*, at 49.
34. Ibid.
35. At 1249.
36. Law Commission (2002). *Defamation and the Internet: A preliminary investigation*, Study No. 2, December 2002, London, from http://www.lawcom.gov.uk/files/deformation2.pdf
37. See http://www.theregister.co.uk/2008/05/27/internet_censorship/ and Giordano, P. (1998). Invoking law as a basis for identity in cyberspace. In L. Ellison & Akdeniz Y., Cyber-stalking: The regulation of harassment on the Internet. *Criminal Law Review* (December Special Edition), *Crime, Criminal Justice and the Internet*, 29–48.

38. See http://radar.oreilly.com/2007/04/draft-bloggers-code-of-conduct.html
39. See e.g. the conviction of Paul Gadd (Gary Glitter) in November 1999 for possession of child pornography.
40. Basu, S., & Jones, R. (2007). Regulating cyberstalking. *Journal of Information, Law and Technology* (2), 1.
41. Though the Basu & Jones paper focuses more on defining cyberspace and cyberstalking as a substantively different behavioural pattern to 'real world' stalking, rather than considering the application of the current legal framework in England and Wales to what the authors of this paper consider to be broadly the same behaviour, though via a modern platform.
42. Williams, M. (2004). The language of cybercrime. In D. Wall (Ed.), *Crime and the Internet* (p. 143). London: Routledge.
43. Wacks, R. (1998). Privacy in cyberspace: Personal information, free speech and the Internet. In L. Ellison & Y. Akdeniz, pp. 29–48.
44. Orlowski, A. (3 April 2004). *Google mail is evil*. Retrieved September 2008, from http://www.theregister.co.uk/2004/04/03/google_mail_is_evil_privacy/
45. See http://www.cyberslapp.org/ for a database of such cases in the USA.
46. [2008] EWHC 687 (QB).
47. See http://www.haltabuse.org
48. See http://www.haltabuse.org/resources/stats/Cumulative2000–2007.pdf
49. See e.g. Wafa, T. (2008). *Internet privacy rights – Global Internet privacy rights: A pragmatic legal perspective*. Available at http://works.bepress.com/tim_wafa/1
50. See e.g. http://www.wikihow.com/Trace-an-IP-Address, and http://www.abika.com/Reports/verifyemail.htm for typical websites.
51. See http://en.wikipedia.org/wiki/Anonymizer
52. For a full report of the circumstances, see http://www.dailymail.co.uk/femail/article-480798/How-barrister-forged-evidence-husband-faces-jail.html
53. See e.g. http://www.eff.org/, the Electronic Frontier Foundation, a not-for-profit organisation dedicated, amongst other things, to preserving free speech on the Internet.
54. See e.g. http://www.greatfirewallofchina.org/
55. 929 F Supp 824 (1996), at p. 883. In Ellison, L., & Akdeniz, Y., 29–48.
56. Nicol, A., QC, Millar, G., QC, & Sharland, A. (in press). *Media Law and Human Rights*, OUP.
57. A Non-Molestation Order in and of itself is not appropriate in all circumstances, as it is limited to 'associated persons' as defined in Section 62(3), being (in the main) partners or ex partners, relatives or persons having had an intimate personal relationship of significant duration.
58. Cal. Civil Code § 1708.7.
59. See http://www.flsenate.gov/Session/index.cfm?Mode=Bills&Submenu=1&BI_Mode=ViewBillInfo&Billnum=0479&Year=2003
60. Knaggs, T., Searle, W., & Simonsen, K. (July 2003). *Talking about sentences and crime: The views of people on periodic detention*. Retrieved September 2008, from http://www.justice.govt.nz/pubs/reports/2003/offender-attitudes/index.html
61. A term coined by Shute, S. (2004). The Sexual Offences Act 2003 (4): New Civil Preventative Orders. Criminal Law Review 2004, 417.
62. Ramsey, P. (2008). *The theory of vulnerable autonomy and the legitimacy of the Civil Preventative Order*. LSE Law, Society and Economy Working Paper 1/2008. Retrieved November 2008, from http://www.lse.ac.uk/collections/law/wps/wps.htm
63. Simester, A., & von Hirsch, A. (2006). Regulating offensive conduct through two-step prohibitions. In A. von Hirsch & A. Simester (Eds.), *Incivilities*. Oxford: Hart.