18th BILETA Conference:*Controlling Information in the Online Environment*

April, 2003
QMW, London

Privacy, freedom of expression and CyberSLAPPs: Fostering anonymity on the Internet?

Diane Rowland
University of Wales, Aberystwyth

Introduction

The Council of Europe in its explanatory note to the Draft Declaration on Freedom of Communication on the Internet[1] makes the comment that 'over the past few years there has been a marked tendency by some governments to restrict and control access to the Internet in a manner which is incompatible with international norms on freedom of expression and information.' Many influential legal commentators have advocated the necessity both for protecting the individual in their private life and at the same time fostering democratic participation and robust public debate by ensuring that those who do participate are protected from stigmatisation, victimisation and embarrassment. However the practical difficulties in determining the scope of a particular right in the face of legitimate and compelling public, societal or governmental interests can be immense. This is even more so when the respective demands of individual rights themselves conflict as can be the case in relation to freedom of expression and privacy.

The advent of the internet, judicially described as a 'truly democratic forum of communication'[2] and 'the most participatory marketplace of mass speech'[3] has meant that the possibility of such active participation has been made a practical reality for more individuals than ever before. Notwithstanding the fact that in some respects there can be a tension between the rights of freedom of expression and the right of
privacy[4], the ease of remaining anonymous (or adopting a pseudonym or pseudonyms) on the internet can help in ensuring that both rights are not eroded. On the other hand, it is also clear that anonymity can allow those who wish to engage in malicious, defamatory or criminal activities to do so with impunity. This paper concentrates not so much on the nature of the content whether expressed or kept private but rather on the legitimacy of techniques used to assist in the protection of freedom of expression and privacy.

The 'problem' areas – the advantages and disadvantages of anonymity and pseudonymity on-line.

There are a number of issues which arise out of the use of anonymity and lead to clashes between either individual rights or the practice of an individual right in the opposition to an allegedly overriding public, governmental or societal interest. An obvious example is the potential for a clash of interests between the right to privacy and freedom of expression. An example is found in the recent case of *A v B and C*[5] which concerned a footballer's attempts to stop publication of revelations about affairs which he had had with two women, the details of which were freely given to

a national newspaper by the women concerned. The Court of Appeal held that A's ability to keep the information private was necessarily restricted by the fact that the women had chosen to reveal the information, otherwise there would be no acknowledgement of their right to freedom of expression. On the other hand, it is without doubt that anonymity safeguards privacy and also safeguards freedom of expression. Many dissidents in oppressive regimes have found that they can only express their views safely[6] behind the shield of anonymity and even within an elected democracy, those who espouse views unpopular with the majority or even a powerful minority may prefer to shelter behind anonymity to avoid reprisals or even merely to ensure that the views expressed are not prejudged on the basis of the identity of the speaker.

The use of anonymity may impede criminal investigations. For some reason, perhaps the threat of almost unbounded damage[7], this seems to be far more of an issue in relation to anonymity on the internet as pointed out by the US Attorney General, John Ashcroft[8] 'attacks on networks, frauds, software piracy, corporate espionage and trafficking in child pornography are just some of the crimes facilitated by the Internet ... it is easy for a criminal to create a fictitious identity to perpetrate frauds, extortions and other crimes ... this anonymity can significantly complicate an investigation.' While not denying the truth in this statement, it is difficult to assess the extent of criminal use as a proportion of total Internet traffic in order to evaluate the justification for denying the benefits of anonymity to innocent users.

A related concern and of particular pertinence since September 11, the instigation of the 'war' on terrorism and the actual war in Iraq is the fear that the Internet provides a perfect communication tool for terrorists. Not only is it global in its reach but it can provide perfect security and secrecy behind a cloak of anonymity. In addition the fear of cyberterrorism where computer networks are themselves both the tools of terrorism and their targets provides another rationale for intervention and regulation.

A right to be anonymous?

The US Supreme Court has considered the use of anonymity in the context of the guarantee of first amendment rights on several occasions. It was discussed in terms of the related right of freedom of association in *NAACP v Alabama*[9] and *Bates v Little Rock*[10] both of which concerned the rights of members of the National Association for the Advancement of Coloured People not to be identified as such. In *Talley v California*[11] in upholding the right to remain anonymous as an essential part of or adjunct to freedom of expression, it was pointed out that the reason for the decision in both *NAACP* and *Bates* was that 'identification and fear of reprisal might deter perfectly peaceful discussions of public matters of importance' and that 'persecuted groups and sects from time to time though out history have been able to criticize oppressive practices and laws either anonymously or **not at all**'[12]. The case concerned a challenge to a Californian law which proscribed the distribution of pamphlets anonymously, the purpose of the legislation being to prevent 'fraud, deceit, false advertising, negligent use of words, obscenity and libel'. It was, in other words, an attempt to use the law proactively as a preventive measure and in this context the views of Clark J, dissenting, are interesting. He felt that the interests of the public in enforcement had to be weighed against the right of Talley and was not convinced that he would suffer any injury by being identified. If this was the case his freedom of expression was not actually restricted which Clark felt was a necessary prerequisite if the legislation was to be struck down. He asserted however that he stood 'second to none in supporting Talley's right of free speech – but not his freedom of anonymity'. This is of course to neglect Talley's or any other person affected by the legislation subjective view that there freedom of expression had in fact been inhibited because they could not express their views anonymously.

The Supreme Court reached a similar decision in the later case of *McIntyre v Ohio*[13], which, like *Talley* concerned a pamphlet distributed anonymously. The court noted that 'the decision in favour of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism or merely by a desire to preserve as much of one's privacy as possible' and went on to find

that the public interest in anonymity unquestionably outweighed the public interest in disclosure and that this extended beyond purely literary works. As in *Talley*, one of the declared aims of the Ohio provision was to combat fraud on which the court's opinion was that
'[Ohio] cannot seek to punish fraud indirectly by indiscriminately outlawing a category of speech based on its content with no necessary relationship to the danger sought to be prevented. One would be hard pressed to think of a better example of the pitfalls of Ohio's blunderbuss approach than the facts of the case before us.'

The court noted that a perpetrator of fraud could easily evade the penalties in the statute by providing a false name as there was no provision requiring authentication. The dissenting judgment of Scalia J however points out that anonymity 'facilitates wrong by eliminating accountability which is ordinarily the very purpose of anonymity' – a view which would certainly have resonance for those who criticise the widespread use of anonymity on the internet.

The subject has been discussed most recently in *Watchtower Bible v Stratton[14]* where the Supreme Court essentially reiterated its existing stance that the right to speak anonymously is a necessary adjunct to freedom of expression as stated by the court in the earlier cases such as *Talley*, above. The small village of Stratton sought to protect its residents from intrusions caused by door to door campaigning and such like by requiring that all those who wished to engage in such activities must register and obtain a permit. The objective was to prevent fraud and crime and protect its citizens' privacy. As in the previous cases, the court found that the ordinance had an undesirably restrictive effect on innocent speech, that criminals would not in any case be deterred by the absence of a permit and that, in relation to privacy, 'the annoyance caused by an uninvited knock on the front door is the same whether or not the visitor is armed with a permit.'

In these cases, the Supreme Court has expressly acknowledged that those who hold unpopular opinions may need the protection of anonymity against those who strongly disagree with them whether private parties or even the government. Presumably this line of reasoning will continue post September 11th and now during the war in Iraq and at least one American politician has recognised that legislative enactments such as the US PATRIOT Act 'increase the opportunity for law enforcement and the intelligence community to return to an era where they monitored and sometimes harassed individuals who were merely exercising their First Amendment rights. Nothing that occurred on September 11 mandates that we return to such an era.'[15]

Protection for anonymous speech has allowed individuals to be frank in their views not only on political and other public issues but also about public figures themselves. On occasions those in the public eye have alleged that such anonymous comments were defamatory and this has also led to a number of lawsuits where the individuals concerned have brought civil suits in an attempt to uncover the identity of those acting anonymously, so called SLAPP lawsuits[16]. Libellous and defamatory comment is one type of speech which is often thought to be encouraged by the use of anonymous speech but these actions rarely succeed. The view of courts is that, notwithstanding the possibility of defamation, in the absence of blatant injury to reputation, the need to protect First amendment rights takes precedence. Indeed attempts to identify those speaking anonymously appears to imperil the protection offered by the First Amendment to such an extent that some 17 states have enacted anti-SLAPP statutes[17]. This right to anonymity has been expressly applied to the internet in cases such as *John Doe v 2theMart.com Inc [18]* albeit there has been recognition that the protection of first amendment rights has to be balanced against the interests of those seeking to remove the anonymity. Similar litigation to that described above has thus been spawned, sometimes referred to as cyberSLAPPS[19]. Since 1998 there have apparently been over 150 lawsuits filed by American companies against anonymous defendants who have posted allegedly defamatory remarks on the internet[20]. Where there is evidence that defamation can be proved many courts and commentators believe that no different standard should be applied to that which would pertain in ordinary print media but that anonymity should be preserved where necessary to 'foster open communication and robust debate' as pointed out in *2TheMart.com*[21]. In particular the court in *Dendrite* set out a four stage test to assist in determining the balance between the right to anonymous speech protected by

the First Amendment and the opposing right to protection of reputation.

- The anonymous poster must be given due notice of the application to reveal his or her identity, together with a reasonable time to oppose the application.
- Precise details must be given of the statements about which complaint is made.
- There must be evidence to support a prima facie case against the anonymous poster.
- The balance must be made between the right of anonymous speech and the strength of the prima facie case taking into account the need for disclosure of identity for the case to proceed.

However the court pointed out that such a balance could only be made on a case-by case basis and the result has been a certain lack of consistency of approach. Nonetheless it is appears generally that, in the context of civil litigation, the US courts are not taking any different approach to the issue of anonymity on-line as providing an essential method of protecting freedom of expression where appropriate. A similar line of reasoning can be identified in *Columbia Insurance Company v Seescandy.com*[22] where the court allowed the registration of domain names pseudonymously.

The situation in the UK is a little different given the absence of a strong tradition of constitutionally protected freedom of speech. Nonetheless the philosopher John Stuart Mill espoused anonymity as a means of protecting free speech and his views are often referred to in the US case law. Despite this there has been no general discussion in the UK courts about the use and abuse of anonymity in this context – perhaps not surprising in a jurisdiction where everything is allowed except that which is forbidden. However the issue was discussed in relation to on-line defamation in *Totalise plc v Motley Fool Ltd*[23]. In this case, the court decided that the balance of interests lay with the removal of anonymity as a strong prima facie case of serious defamation had been made which could result in significant damage given the potentially vast audience on the Internet and that there was no other way of identifying the alleged defamer. Owen J had 'no hesitation' in arriving at this conclusion since when balancing the requisite interests 'the respect for and the protection of the privacy of those who choose to air their views in the most public of for a must take second place to the obligation imposed upon those who become involved in the tortuous acts of others to assist the party injured by those acts'. Although couched in rather different language, this outcome is probably not radically different from that which would be arrived at by a US court in similar circumstances.

The UK courts have also had reason to consider the clash between privacy and freedom of expression in a rather different context, that of data protection. Article 9 Data Protection Directive [24] which provides for exemptions or derogations from the usual data protection rules for journalistic, artistic or literary expression only (the so-called special purposes) if that is necessary to reconcile the right to privacy with freedom of expression. This has been implemented in the UK by s32 Data Protection Act 1998 and was recently considered at length by the Court of Appeal in *Campbell v Mirror Group Newspapers*.[25] Much of this discussion is of a technical nature concerning the detailed interpretation of the various sub-sections, although the case concerned Naomi Campbell's right to privacy rather than any specific issue relating to anonymity, it does demonstrate the approach of the court to balancing competing interests, both in terms of individual rights and in the wider public interest.

Anonymity and Privacy

Regulatory techniques including the law on data protection are not completely effective in protecting privacy on-line and the scope for their application to global networks such as the internet is uncertain. Anonymity is also an important method, perhaps the only reliable method, of protecting privacy on-line and has been recommended in the context of e-commerce by both the OECD and the Council of Europe subject to appropriate safeguards[26]. But it is clear that anonymity can be used for good and bad and, before anonymity is espoused as a panacea for all privacy problems, a balance must be found between its beneficial effects in enhancing both privacy protection and freedom of speech and its potential disadvantages specifically the facilitation of anti-social and illicit activities.

Further, there needs to be some estimate of the magnitude of the potential problem on both sides namely the percentage of activities which may pose a threat to privacy compared to the volume of criminal activity together with the seriousness of the problems of either type i.e. a process akin to risk assessment. There are many unknowns (and perhaps unmeasurables) here but there is a very real danger of putting forward a solution without any realistic measure of either the likely success or even the potential harm or a serious consideration and evaluation of alternatives. At the end of the twentieth century it appeared that the organisations making recommendations in this area had accepted that balancing the risks involved led to a result which tended to favour the preservation of anonymity or perhaps the use of traceable pseudonymity notwithstanding the unpopularity of these views amongst law enforcement agencies. But attitudes have changed after September 11th and the pendulum may now be swinging in the opposite direction as a reaction to recent world events and justified on the basis of the war against terrorism and extended to include illicit activities more generally.[27]

The 'real world' analogy – should the same standard be applied on and off-line?

In the report of the President's working group on unlawful conduct on the internet[28] a constant theme is to apply the same standards on-line as are applied off-line and this is reiterated in the Council of Europe draft declaration referred to earlier. The reality however is that the analogy between real space and Cyberspace is not a perfect one. So although this might be a justifiable starting point it should not necessarily be regarded as an automatic finishing point. There are significant differences between real space and cyberspace which could affect both the manifestation of anonymity on-line and off-line and which therefore may have an impact on the appropriate balance of rights. To what extent might these differences of both quality and quantity be crucial in deciding whether these differences are sufficiently material to warrant a difference in standards? The true meaning of anonymity is lacking a name but this has also been extended to lacking distinctive features or individuality but should arguably not extend to the lack of identity as such. In real life it is possible to identify people without knowing their name, but this need not extend to knowing anything else about their characteristics. On the other hand on the internet, participants in a chat room, for instance, may have no knowledge of the actual names or characteristics of others on-line but yet can 'identify' them from their known characteristics (these could be quite different to those which they exhibit in the real world[29]) which relate only to a pseudonym and there is the very real possibility that one single person may be using several pseudonyms. Although someone in real life can assume several identities there are real limits to the range of possible identities – this is not such a problem on the internet. But on the internet as in real life the larger the community, the less likely it is that someone will be identified. These nuances of meaning (which could be attacked perhaps as a trivial argument of semantics) show that there are some occasions on which only the protection afforded by anonymity will protect the individual.

Conclusions

As shown above the analogy between activity in the real world and in Cyberspace is by no means a perfect one and the extent of the divergence should be taken into account in any proposals to limit the use and therefore the protection afforded to individual rights by the ability to remain anonymous. In respect of privacy, it is the case that surveillance of Internet use may be considerably easier than surveillance of activities in the real world. On the other hand, using technological means such as encryption and anonymising software, it is possible to use the Internet both without being identified and without the interceptor being able to view the contents of the communication. It is much more difficult in the real world to avoid being at least identifiable, even if technically still anonymous. However day to day real world surveillance in the form of CCTV etc. has to conform to a Code of Practice[30] which includes a requirement of warnings and so on – surveillance of internet use is likely to be a much more covert activity even if the user is aware that it may occur or that there is a power to do so. Anonymity has been espoused by various international and intergovernmental organisations as a suitable tool for protecting the privacy of consumers in relation to e-commerce.

Interestingly although arguably such consumers might also be able to browse in shopping malls anonymously in real life they would nevertheless be likely to remain identifiable.

In my 2000 Bileta paper[31] I suggested that traceable pseudonymity was capable of balancing all of these factors in principle and that there was no greater threat that could only be satisfactorily dealt with by the assurance of complete anonymity. Since then the political climate has polarised and this may now represent an over-generalisation. Unlike anonymity, traceable pseudonymity requires some agreed scheme with certain bodies who would then retain the true identities of those using pseudonyms. However it is arguable whether such a scheme would or could be workable in practice. There are too many technological ways by which the average internet user can send anonymous mail or can avail themselves of a pseudonym and there is little incentive to comply with a prescribed scheme, whether or not it purports to be mandatory. Identity checks, even geographical location, on-line are notoriously difficult to implement. However Governments are increasingly nervous of anonymous/pseudonymous traffic on the internet and conversely users are increasingly nervous of governments using their powers to intercept and force identification of those who attempt to hide behind a cloak of anonymity for good or bad reason.

Principle 7 of the Council of Europe draft declaration concerns the right to remain anonymous for reasons connected with both privacy and freedom of expression:

> In order to ensure protection against on-line surveillance and to enhance the free expression of information and ideas, Member States should respect the will of users of the internet not to disclose their identity. This does not prevent member States from taking measures and co-operating in order to trace those responsible for criminal deeds ...'

The two-fold protection which this offers ensures both that freedom of expression is not unnecessarily inhibited and also that society is not deprived of potentially valuable information and ideas, and also that users are safeguarded against unwarranted on-line surveillance by public or private entities. The consequence of this is that the use of anonymity tools and software should not be restricted without just cause i.e. any action taken should be proportional to the risk (taking account also perhaps of elements related to the perceived risk). One problem which may merit further investigation is the relative effectiveness of proactive and reactive measures in this regard. Whereas in some areas of law, provisions only provide a remedy after the event there is a growing trend, often in relation to activities perceived as 'high risk', to try and address the matter at source with more proactive provisions. These are far more difficult to formulate, apply and enforce and unless proportional to the actual risk are likely to affect adversely the law-abiding user without necessarily providing any adequate control of the risk originally identified. It was this type of reaction which led to the type of 'blunderbuss' approach referred to in *McIntyre v Ohio*[32]. There are many millions of users of the internet and it is likely that the percentage of those who would abuse its resources is relatively small such that it may be unnecessary to resort to such tactics. If this is the case then there is no reason why anonymity should not be the default for most applications if desired.

---

[1] CDMM (2002) Misc18 29 November 2002.
[2] *Doe v 2theMart.com Inc* 140 F Supp 2d 1088, 1097.
[3] 929 F Supp 824, 881 (ED Pa 1996).
[4] See e.g. Directive 95/46EC Article 9, Data Protection Act 1998 s32 and discussion in *Campbell v*

Mirror Group Newspapers [2002] EWCA Civ 1373 and [2002] EMLR 30 (QBD).
[5] [2002] 3 WLR 542, [2002] 2 All ER 545.
[6] See e.g. Yaman Akdeniz 'Anonymity, Democracy and Cyberspace' (2002) 69 Social Research 223, 224.
[7] The 'Melissa' virus, for instance, has been estimated to have cost $80m of damage and the 'iloveyou' virus has been described as 'perhaps the most devastating crime in history' in terms of the damage done and the number of people affected. See e.g. Neal Kumar Katyal 'Criminal Law in Cyberspace' (2001) 149 U Pa L rev 1003.
[8] First Annual Computer Privacy, Policy and Security Institute May 22, 2001 available at www.usdoj.gov/criminal/cybercrime/AGCPPSI.htm.
[9] 357 US 449, 2 L Ed 2d 1488 (1958).
[10] 361 US 516, 4 L Ed 2d 480 (1960).
[11] 4 L Ed 2d 559 (1960).
[12] ibid at 563, my emphasis.
[13] 514 US 334, 131 L Ed 2d 426 (1996).
[14] 153 L Ed 2d 205 (2002).
[15] John Podesta, White House Chief of Staff, 1998-2001 quoted in www.epic.org/privacy/terrorism/usapatriot.
[16] Strategic lawsuits against public participation.
[17] See Shaun B Spencer 'CyberSLAPP suits and John Doe subpoenas: Balancing anonymity and accountability in Cyberspace' (2001) 19 J Marshall J Computer & Info L 493.
[18] 140 F Supp 2d 1088 (2001).
[19] See e.g. *John Doe v 2theMart.com Inc* (above), *Dendrite International Inc v John Doe* 775 A 2d 756 (2001) and cf. *Totalise plc v Motley Fool Ltd* The Times 15 March 2001. [20] David C Scileppi 'Anonymous Corporate Defamation Plaintiffs: Trampling the First Amendment or Protecting the Rights of Litigants' (2002) 53 Fla L Rev 333.
[21] 140 F Supp 2d 1088 and see also discussion in Jennifer O'Brien 'Putting a face to a (screen) name: the First Amendment implications of compelling ISPs to reveal the identities of anonymous internet speakers in online defamation cases' (2002) 70 FDMLR 2745.
[22] 185 FRD 573 (1999).
[23] above n.17.
[24] Directive 95/46/EC.
[25] [2003] 2 WLR 80, [2003] 1 All ER 224.
[26] See e.g. Diane Rowland 'Anonymity, Privacy and Cyberspace' www.bileta.ac.uk/00papers/rowland.html.
[27] For a report on relevant legislative activity since September 11th see e.g. 'The Internet on probation' www.gipiproject.org/content/int-probation.pdf.
[28] 'The Electronic Frontier: the challenge of unlawful conduct involving the use of the internet' March 2000 www.usdoj.gov/criminal/cybercrime/unlawful.htm.
[29] See also discussion of deindividuation in the internet context in Rowland, D 'Anonymity, Privacy and Cyberspace' 15th Annual BILETA Conference, Warwick April 2000 www.bileta.ac.uk/00papers/rowland.html.
[30] Available from www.dataprotection.gov.uk/dpr/dpdoc.nsf.
[31] ibid.
[32] Above n. 12.