

Online anonymity: some legal issues

Recent developments in online defamation and copyright infringement have led to increased interest in online anonymity. Plaintiffs now have to consider how they might go about identifying defendants known only by a pseudonym or possibly only a computer address. This article discusses the ways in which plaintiffs can seek assistance in identifying anonymous defendants, particularly in relation to compelling Internet Service Providers to reveal the identity of their subscribers.

Introduction

The Internet is uniquely suited to anonymous or pseudonymous communication. Online users can choose how much information about themselves will be given out—they may choose to remain anonymous, or they may choose to shelter behind a pseudonym.¹ Indeed, in the early years of the medium there was (and to some extent there still is) a widespread belief that Internet use was essentially untraceable—a belief summed up in the famous New Yorker cartoon which showed two dogs sitting in front of a computer with one saying to the other, “On the Internet no one knows you’re a dog”.²

This has had mixed effects. On the one hand, anonymous communications can promote communication, for example, by encouraging candour, facilitating discussion of unpopular views, and enabling whistleblowers to reveal impropriety without fear of retaliation.³ On the other hand, anonymity can encourage wrongdoing and in particular create a perception that the user cannot be held accountable for his or her actions or words. There have been a number of cases in Ireland where individuals have set out to systematically smear or harass others by means of the Internet (including two particularly serious cases where convictions for criminal libel resulted) apparently believing that anonymous postings could not be traced to them.⁴

More recently, though, it has become clear that Internet use will, unless the user is both technically skilled and very careful, leave a trail of digital

footprints. Lloyd points out that:

“Even the Internet and WWW, which are often touted as the last refuge of individualism, might equally be described as a surveillance system par excellence. E-mail messages may be copied many times in the course of transmission and remain on a variety of servers. An individual browsing the web leaves electronic trails where he or she passes. A software program [*sic*] known as a ‘cookie’ may be transmitted from a website to the user’s computer and remain there until the site is next accessed, at which time details of the user and previous visits to the site will automatically be transmitted.”⁵

Consequently, it is often possible to identify a user, even though that user might have attempted to conceal or disguise his identity. Generally, however, identification will require co-operation from third parties, such as the user’s Internet Service Provider (“ISP”). This article therefore explores the legal issues surrounding attempts by plaintiffs to identify alleged wrongdoers, and in particular the extent to which third parties such as ISPs can be compelled to reveal the identities of their users.

Background: From the ISP to the individual defendant

Litigation seeking the identity of Internet users is a comparatively new development. There has been no Irish case on point, while the first significant United States decision⁶ dates from 1999 and the first English decision from 2001.⁷ It seems that, until recently, litigants faced with anonymous defendants generally pursued ISPs directly, rather than deal with the uncertainties of putting a name to the defendant. Sullivan puts it well when he states that:

“Defamation suits may be about deterrence, but they are also about money, which makes ISPs logical targets. Indeed, the first generation of internet libel actions sought to impose liability on ISPs for defamatory material posted by their subscribers. By suing an ISP, plaintiffs are not only able to side-step the time and expense associated with discovering the identity of the person who posted the message, but they also increase their chances of getting paid.”⁸

However, this approach is now much less attractive for plaintiffs, since most jurisdictions have now

TJMcIntyre
B.C.L., LL.M, B.L.,
Lecturer-in-Law,
University College
Dublin.

¹ See Lee, “Addressing Anonymous Messages in Cyberspace” (1996) 2 (1) *Journal of Computer-Mediated Communication*, <http://www.ascusc.org/jcmc/vol2/issue1/anon.html>.

² The cartoon, by Peter Steiner in 1993, is available at <http://www.unc.edu/depts/jomc/academics/dri/idog.html>.

³ For examples, see Lee, *op cit*.

⁴ Cunneen, “Surfing for Slander”, *The Sunday Business Post*, May 6, 2001; O’Driscoll and Mac Ruairí, “Man Jailed for Libel on the Internet”, *Irish Examiner*, December 21, 1999.

⁵ *Information Technology Law* (3rd ed., Butterworths, 2000), p.35.

⁶ *Columbia Insurance Co. v Seescandy.com* 185 F.R.D. 573 (N.D. Cal. 1999).

⁷ *Totalise plc v The Motley Fool Ltd.* [2001] E.M.L.R. 29.

⁸ Sullivan, “In Search of John Doe: Piercing the Veil of Anonymity on the Internet” (2002) 13 (1) *Entertainment L. Rev.* 21.

enacted legislation conferring immunities on ISPs and other Internet intermediaries.⁹

Another development, this time technological rather than legal, has also led to an increased focus on individual users. The growth of file sharing (particularly of music in MP3 format) has led to much litigation from copyright holders alleging an infringement of their rights. Early file sharing services (such as Napster, or Audiogalaxy) were centralised in nature and depended on a master index maintained on a central server. This provided a single, inviting target for litigants—succeed in taking down the central server and the service ceases to exist.¹⁰

Unfortunately (from the point of view of plaintiffs), a second wave of file sharing services has since sprung up which are decentralised in nature. Services such as KaZaA or Gnutella are described as peer-to-peer (P2P), reflecting the fact that they are self-organising and do not depend on central administration. This means that litigants have no easy targets—even if the company behind the software is shut down, users can continue sharing files without noticing any change.

Consequently, plaintiffs increasingly have to focus on suing individual users.¹¹ This can already be seen in the United States, where the Recording Industry Association of America (RIAA) has launched¹² a nationwide campaign of litigation against file sharers while its international counterpart, the International Federation of the Phonographic Industry (IFPI), has recently commenced litigation in Denmark, Germany, Italy and Canada.¹³ We can, therefore, soon expect to see more cases where plaintiffs seek to identify the users of peer-to-peer services.

Voluntary disclosure?

A litigant's first step, having traced a user as far as a particular ISP or other intermediary, will no doubt be to ask for voluntary disclosure of the user's identity. May the ISP or intermediary choose to make such disclosure?

Under the Data Protection Acts 1988 and 2003, the identity of the user will amount to personal data, and as such disclosure will generally not be permissible unless the user consents, or one of the other exemptions in s.2A can be relied upon.

The ISP may have dealt with this issue in its Acceptable Use Policy (AUP) or other terms of use. If so, no difficulty is presented since the user will have consented to disclosure as contemplated by the AUP.

An example can be seen in the General Terms and Conditions of the Vodafone Ireland website,¹⁴ which states that:

“Vodafone will not disclose to third parties any personal information about you or your use of the Services without your prior permission unless Vodafone has a good faith belief that such action is necessary to: ... (4) act to protect the interests of third parties.”

An appropriately drafted AUP should, therefore, provide for consent to voluntary disclosure thus avoiding any problems for the ISP.¹⁵

Absent such an AUP, the only relevant exemption would appear to be that in s.2A(1)(d), under which personal data can be disclosed where this is:

“necessary for the purposes of the legitimate interests pursued by the data controller or by a third party or parties to whom the data are disclosed, except where the [disclosure] is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject.”

This is a relatively narrow exemption which will permit (but not require) voluntary disclosure to a person seeking to identify an alleged wrongdoer, subject to tests of necessity and proportionality. It is likely, however, to place an ISP which relies on it in a difficult, quasi-judicial position.

As regards necessity, the ISP would have to consider whether the litigant could pursue his legitimate interests only if the identity of the user is revealed. If, for example, the litigant might have other remedies open to him, then disclosure might be said to be unnecessary. Similarly, as regards proportionality, the ISP would have to consider whether the legitimate interests of the litigant in identifying the user were outweighed by the prejudice which disclosure would cause to the user.

How an ISP is to acquire the information necessary to apply these tests is unclear. The only obvious means of doing so would be to invite both the litigant and the user to make representations. The ISP is unlikely to relish carrying out this cumbersome process. Similarly, the ISP is unlikely to relish the application of the balancing test which the exemption applies, given its likely lack of any special expertise in

⁹ The United States led this trend with s.230 of the Communications Decency Act 1996, while at European Union level the most significant development has been Art.4 of the E Commerce Directive (Directive 2000/31/EC).

¹⁰ Massey, “Spelling the End for Napster” (2001) 12 Entertainment L. Rev. 249.

¹¹ Stokes and Rudkin-Binks, “Online Music – P2P Aftershocks” (2003) 14 Entertainment L. Rev. 127.

¹² *ibid.*

¹³ Oates, “Music biz takes P2P jihad to Europe and Canada”, *The Register*, March 30, 2004, http://www.theregister.co.uk/2004/03/30/music_biz_takes_p2p_jihad/.

¹⁴ <http://www.vodafone.ie/terms/website/index.jsp>.

¹⁵ Assuming that the consent is, as required by of the Directive, “freely given, specific and informed” (Art.2(h)), and “unambiguous” (Art.7(a)). On this point, see Jay and Hamilton, *Data Protection Law and Practice* (2nd ed, Sweet & Maxwell, 2003), pp.90–94. An AUP may not amount to valid consent if, for example, it is not given sufficient prominence to bring it to the attention of users.

the area, and the possibility of being found liable to the user if a court later finds that disclosure was unwarranted.

There are, therefore, more kicks than pence for the ISP in relying on the exemption, and in most cases the ISP would appear to be better off simply to refuse voluntary disclosure.

This conclusion is reinforced by the only case on point, the English decision in *Totalise plc v The Motley Fool*.¹⁶ In that case, two defendants operated websites which included discussion boards for business information. A user under the name of “Z Dust” made various defamatory postings concerning the plaintiff firm. The plaintiff contacted the defendants seeking to have the postings removed, the user’s rights revoked, and the identify of the user revealed. Both defendants declined to reveal the identity of the user without a court order to that effect, relying on the combined effect of their own privacy policies and the Data Protection Act. Both defendants were ultimately ordered to reveal the identity of the user (by way of a *Norwich Pharmacal*¹⁷ order, discussed further below), but in deciding whether to fix the defendants with the costs of that action, the court had to consider whether they could or should have made disclosure voluntarily.

The plaintiff argued that costs should lie against the defendants, on the basis that they should have made voluntary disclosure under s.35(2) and Condition 6, Sch.2 of the Data Protection Act 1998 (which is identical with the s.2A(1)(d) exemption under the Irish Act¹⁸), and the High Court (Owen J.) agreed, stating that:

“[I]t was perfectly plain from the outset that the postings on both websites were highly defamatory and that, accordingly, the claimants were the victims of a sustained campaign amounting to an actionable tort. There was no other way in which the claimants could have proceeded, save by requiring identification of Z Dust from both defendants.

I accept that the defendants had to carry out the balancing exercise, but in my judgment there was only one answer to the balancing exercise, namely that they should have complied with the requests made by the claimant.”

On appeal by the second defendant, the Court of Appeal reversed that aspect of the decision. It accepted that voluntary disclosure was possible under the Data Protection Act 1998, subject to a balancing test. However, the court went on to make it clear that the mere existence of a non-disclosure exemption did not oblige the defendant to make the requested disclosure.

It also took the view that the second defendant acted entirely correctly in refusing disclosure.

“[Counsel for the claimant] has suggested that the issue need never come before a court: an intermediate party asked to disclose someone’s identity can perfectly well act on their lawyer’s advice as to what the likely outcome in court would be, and can look to the claimant for the cost of obtaining the advice. We doubt this. There are many factors which are material to enforced disclosure ... It is perfectly possible, for example, that a judge would refuse disclosure of the identity of a data subject whose attacks, though legally defamatory, were visibly the product of a deranged mind, or were so obviously designed merely to insult as not to carry a realistic risk of doing the claimant quantifiable harm.

We also believe that it is legitimate for a party ... who reasonably agrees to keep information confidential and private to refuse to voluntarily hand over such information ... [W]e are not convinced that Interactive were free to hand over the information without coming to a view on the merits. That was not their task.”¹⁹

This decision confirms the conclusion that, while voluntary disclosure may be possible under s.2A(1)(d), in practice there will be little incentive for ISPs to make such disclosure, particularly where it will involve carrying out a difficult balancing exercise with possible exposure to liability.²⁰

Compelling disclosure

The Norwich Pharmacal / Megaleasing jurisdiction
Where voluntary disclosure is refused, the plaintiff may seek to compel disclosure by way of the jurisdiction established in *Norwich Pharmacal v Customs and Excise*.²¹ That jurisdiction, approved of in Ireland by *Megaleasing (UK) Limited v Barrett*²² allows the court to order a third party to reveal the identity of a wrongdoer where that third party has become “mixed up” in the tortious acts of another through no fault of its own.

This jurisdiction is equitable in nature—as such, the order is discretionary, and the court is free to consider all the relevant circumstances in exercising that discretion. Some relevant circumstances were set out in *Norwich Pharmacal* itself, in particular whether disclosure would be contrary to the public interest:

¹⁹ *Totalise plc v The Motley Fool* [2002] 1 W.L.R. 1233 (C.A.), per Aldous L.J.

²⁰ See the discussion in Jay and Hamilton, *Data Protection Law and Practice* (2nd ed, Sweet & Maxwell, 2003), pp.437–438.

²¹ [1974] A.C. 133.

²² [1993] I.L.R.M. 497.

¹⁶ [2001] E.M.L.R. 29 (H.C.); [2002] 1 W.L.R. 1233 (C.A.).

¹⁷ *Norwich Pharmacal v Commissioners for Customs and Excise* [1974] A.C. 133.

¹⁸ Both acts simply transcribe Art.7 of the Data Protection Directive (Directive 95/46/EC) *verbatim*.

“[s]uch matters as the strength of the applicant’s case against the unknown alleged wrongdoer, the relation subsisting between the alleged wrongdoer and the respondent, whether the information could be obtained from another source, and whether the giving of the information would put the respondent to trouble which could not be compensated by the payment of all expenses by the applicant”.²³

This jurisdiction was applied to anonymous Internet users in *Totalise plc v The Motley Fool*,²⁴ the facts of which are set out above. In that case, the High Court and the Court of Appeal took somewhat different views as to how the *Norwich Pharmacal* principles should apply in an Internet context.

Owen J. in the High Court held that there was no doubt but that disclosure was appropriate, and gave short shrift to the privacy concerns raised by the defendants:

“I turn then to the exercise of my discretion to grant the relief sought. I am satisfied, first, that much of the content of the Z Dust postings on both defendants’ discussion boards is plainly defamatory. Defamation is a tort of strict liability. The claimant has demonstrated a strong prima facie case against Z Dust. Secondly, the defamatory material is of a very serious nature, calling into question the claimant’s solvency and the competence and integrity of its management and directors. Third, the concerted campaign waged by Z Dust presents a very considerable threat to the claimant. The potential audience is vast. It has no geographic limit. The claimant, in my judgment, is at risk of serious damage. Fourth, Z Dust is hiding behind the anonymity afforded by access to the defendants’ discussion boards. Fifth, the claimant has no other practical means of identifying Z Dust ... [W]hen balancing the interests of the parties, the respect for and protection of those who choose to air their views in the most public of fora must take second place to the obligation imposed upon those who become involved in the tortious acts of others to assist the party injured by those acts.”

Aldous L.J., for the Court of Appeal, sounded a more cautious note, however, pointing out that:

“In a case such as the present, and particularly since the coming in force on 2 October 2000 of the Human Rights Act 1998, the court must be careful not to make an order which unjustifiably invades the right of an individual to respect for his private life, especially when that individual is in the nature of things not before

the court: see the Human Rights Act, 1998, section 6, and the European Convention on Human Rights, Articles 10 and (arguably at least) 6(1). There is nothing in Article 10 which supports [counsel’s] contention that it protects the named but not the anonymous, and there are many other situations in which – again contrary to [counsel’s] contention – the protection of a person’s identity from disclosure may be legitimate.”

This is a significant passage. The Court of Appeal, unlike the High Court, recognises that anonymity is not merely a mask for wrongdoers, but has social value in its own right. While this stops short of the United States Supreme Court’s ringing endorsement of anonymity (see below) it does accept that there will be situations where the court will be justified in exercising its discretion to refuse disclosure.

In addition, the Court of Appeal criticised the procedure behind the application, and suggested that the user should be put on notice of the application and given an opportunity to put his case before the court.

“It is difficult to see how the court can carry out this task [*i.e. decide on disclosure*] if what it is refereeing is a contest between two parties, neither of whom is the person most concerned, the data subject; one of whom is the data subject’s prospective antagonist; and the other of whom knows the data subject’s identity, has undertaken to keep it confidential so far as the law permits, and would like to get out of the cross-fire as rapidly and as cheaply as possible. However, the website operator can, where appropriate, tell the user what is going on and offer to pass on in writing to the claimant and the court any worthwhile reason the user wants to put forward for not having his or her identity disclosed. Further, the court could require that to be done before making an order. Doing so will enable the court to do what is required of it with slightly more confidence that it is respecting the law laid down in more than one statute by Parliament and doing no injustice to a third party, in particular not violating his convention rights.”²⁵

This discussion will apply with equal force in this jurisdiction: where a *Norwich Pharmacal* order is made without giving the user an opportunity to be heard, this may arguably be a breach both of the constitutional guarantee of fair procedures²⁶ and of Art.6 of the European Convention on Human Rights, as implemented by the European Convention on Human Rights Act 2003. There will certainly be situations (akin

²³ [1974] A.C. 133 at 198–199, *per* Lord Cross.

²⁴ [2001] E.M.L.R. 29 (HC); [2002] 1 W.L.R. 1233 (C.A.).

²⁵ *Totalise plc v The Motley Fool* [2002] 1 W.L.R. 1233 (C.A.), *per* Aldous L.J.

²⁶ See, *e.g.*, *Irish Family Planning Association v Ryan* [1979] I.R. 295.

to *Anton Piller*²⁷ scenarios) where putting the user on notice might be inappropriate. However, unless the plaintiff has evidence that harm would be caused by notifying the user, it is submitted that the user should be made aware of the application and be given an opportunity to be heard.

Canadian developments

A further application of the *Norwich Pharmacal* principles has recently taken place in Canada. In *BMG Canada Inc. v Doe*,²⁸ the plaintiffs were Canadian recording companies who sought disclosure from Canadian ISPs of the identities of certain users who, they alleged, had infringed copyright laws by trading in downloaded music using peer-to-peer file sharing programs.

The court (von Finckenstein J.) refused to make a *Norwich Pharmacal* order. Two of his findings are of little interest, since they are specific to the facts of the particular case. The plaintiffs had failed to make out a prima facie case against the defendants, and had failed to establish that the ISPs were the only practical source for the identity of the users. The third finding is, however, of more general interest, in that he found that the public interest in disclosure did not outweigh the legitimate privacy concerns of the defendants:

“In this case, the plaintiffs have a legitimate copyright in their works and are entitled to protect it against infringement. However before making the order, the Court evidently must be satisfied that the information about to be disclosed is reliable and should restrict disclosure to the minimum required for the plaintiffs to identify an alleged defendant. Any order made should also, having in mind the privacy interests of the defendants, be accompanied by restrictions and confidentiality orders as the Court sees appropriate. All of the ISPs have indicated that they can produce the required information if requested in a timely fashion. In this case the evidence was gathered in October, November and December 2003. However, the notice of motion requesting disclosure by the ISPs was not filed until February 11, 2004. This clearly makes the information more difficult to obtain, if it can be obtained at all, and decreases its reliability. No explanation was given by the plaintiffs as to why they did not move earlier than February 2004. Under these circumstances, given the age of the data, its unreliability and the serious possibility of an innocent account holder being identified, this Court is of the view that the privacy concerns outweigh the public interest concerns in favour of disclosure.”

This passage illustrates one of the dangers of the *Norwich Pharmacal* order in an Internet context—the information being used is often unreliable, and there is a real risk that innocent users will be identified along with the real targets of the plaintiff. In fact, the campaign of litigation being brought by the RIAA in the United States has already led to a substantial number of false positives, including one well-publicised case of a 66 year old grandmother accused of downloading music by rap artist Snoop Dogg.²⁹ The RIAA’s embarrassment in that case was complete when it was established that the defendant’s computer was not even capable of running the file sharing program (KaZaA) she was alleged to have used.

The United States approach

There have been numerous cases in the United States seeking the identity of anonymous users. In relation to defamation of corporations alone, one writer counts over 150 actions between 1998 and 2002.³⁰ United States courts have therefore rapidly evolved guidelines as to when disclosure is appropriate.

One of the most important aspects of the United States case law is the strong protection the First Amendment of the Constitution gives to anonymous speech. The Supreme Court has held in a number of cases that the right to speak anonymously is an aspect of freedom of expression. See, for example, *McIntyre v Ohio Elections Commission*,³¹ where the court noted that “[u]nder our Constitution, anonymous pamphleteering is not a pernicious, fraudulent practice, but an honourable tradition of advocacy and dissent. Anonymity is a shield from the tyranny of the majority.”³²

This protection of anonymity has been extended to the Internet. In *Columbia Insurance v Seescandy.com*³³ it was recognised that online anonymity:

“can foster open communication and robust debate ... People who have committed no wrong should be able to participate online without fear that someone who wishes to harass or embarrass them can file a frivolous lawsuit and thereby gain the power of the court’s order to discover their identity.”³⁴

Accordingly, United States courts have recognised that special safeguards should apply to the disclosure of users’ identities, lest there be a chilling effect on their First Amendment rights. The leading case is *Dendrite International, Inc. v John Doe No. 3*,³⁵ where the plaintiff firm brought a defamation action against

²⁷ *Anton Piller K.G. v Manufacturing Processes Ltd.* [1976] Ch. 55.

²⁸ [2004] F.C. 488.

²⁹ Schwartz, “She Says She’s No Music Pirate”, *New York Times*, September 25, 2003.

³⁰ Scileppi, “Anonymous Corporate Defamation Plaintiffs: Trampling the First Amendment or Protecting the Rights of Litigants?” (2002) 54 Fla. L. Rev. 333.

³¹ 514 US 334 (1995).

³² 514 US 334 (1995) at 357.

³³ 185 F.R.D. 573 (N.D. Cal. 1999).

³⁴ 185 F.R.D. 573 at 578.

³⁵ 775 A.2d 756 (N.J. App. Div. 2001).

“John Doe” defendants, and sought to have their ISPs identify them. The New Jersey Appellate Division recognised their legitimate interest in doing so, but held that:

“[t]he trial court must consider and decide [this application] by striking a balance between the well-established First Amendment right to speak anonymously, and the right of the plaintiff to protect its proprietary interests and reputation”.³⁶

The court therefore set out a four-part test to determine whether disclosure should be ordered. First, the anonymous user must be given notice of the application (as far as possible) and a reasonable opportunity to oppose it. Secondly, the plaintiff must specify precisely the statements which are alleged to be defamatory. Thirdly, there must be evidence to support a prima facie case against the user. Finally, the court will then balance the interest of the plaintiff in identifying the user against the First Amendment rights of the defendant, taking into account the strength of the plaintiff’s claim.

This is a strict test, placing substantial hurdles in front of plaintiffs. In this case itself, the court declined to order identification, noting that the third part of the test was not met—the plaintiff had merely asserted, without evidence, that the statements made by “John Doe No. 3” had caused harm to it.

On the other hand, this test is far from insurmountable. In *Immunomedics, Inc. v Jean Doe*,³⁷ a companion decision of the same court handed down on the same day, the court accepted that the test had been met. In that case, the anonymous user had posted confidential material on the Internet and appeared to be an employee of the plaintiff. As such, the court found it likely that she was in breach either of her contract of employment or her common law duty of confidentiality, and held that the plaintiff firm had made a sufficiently strong case to justify her identification.

Broadly similar approaches have been taken in other recent United States decisions, including *Doe v 2themart.com*³⁸ and *America Online Ltd. v Anonymous Publicly Traded Corporation*.³⁹

Conclusion

From the above case law we can discern a remarkable degree of consensus between the English, Canadian and United States courts, giving us a number of common themes which are likely to influence an Irish court called upon to make a *Norwich Pharmacal* order against an Internet user.

First, and perhaps most importantly from a practical point of view, there appears to be a general view that the anonymous user should be given an opportunity to make representations to the court before they are

stripped of their anonymity. This could best be done by adopting the procedure suggested in *Totalise plc. v The Motley Fool*,⁴⁰ i.e. requiring the ISP to notify the user, and then allowing the user to make written submissions via the ISP. In addition, the user should (if they wish to instruct lawyers) be given the opportunity to be heard on the application, via a mechanism that will preserve their anonymity. It is submitted that some such procedure must be adopted if the constitutional and European Convention on Human Rights concerns already discussed is to be avoided.

Secondly, the case law recognises that these orders create special concerns from both a privacy and freedom of expression point of view. As such, there is agreement that the plaintiff must show that disclosure is genuinely necessary before an order will be made. It should not be assumed, however, that disclosure is necessary merely because litigation cannot be commenced against the user otherwise. In many cases, it will be open to the plaintiff to pursue other remedies—either litigation against other defendants, or non-litigation remedies such as requiring an ISP to cease hosting a site. If there are adequate alternative remedies open to a plaintiff, it may well be argued that disclosure is not in fact necessary.⁴¹

Thirdly, again related to the privacy and freedom of expression concerns, the case law accepts that the court should engage in a balancing exercise before making disclosure, taking into account factors such as the strength of the plaintiff’s case, the impact which disclosure would have on the user’s rights, the public interest in disclosure or non-disclosure, and any other factors which might be put forward by the user. This approach, if followed here, will give the court a very wide discretion as to the factors which it might take into account. It would appear to be legitimate, for example, for a court to decline to order disclosure, even though a plaintiff has made out a prima facie case, where the injury suffered is trivial, or (as contemplated by *Columbia Insurance v Seescandy.com*⁴² and *Doe v 2themart.com*⁴³) where the plaintiff appears to be motivated primarily by an improper purpose such as a desire to harass or embarrass the user.

Finally, *BMG Canada Inc. v Doe*,⁴⁴ points out that the material held by ISPs will often be unreliable when it comes to identifying a particular user, particularly where the plaintiff has delayed before seeking disclosure. This factor must be borne in mind by the court in exercising its discretion. It would be unjust to subject a user to the expense and inconvenience of defending an action where there is a real risk that the evidence purporting to identify him does not in fact do so.

³⁶ 775 A.2d 756 at 760.

³⁷ 775 A.2d 773 (N.J. App. Div. 2001).

³⁸ 140 F. Supp. 2d. 1088 (2001).

³⁹ 542 S.E. 2d. 377 (Va. 2001).

⁴⁰ [2002] 1 W.L.R. 1233.

⁴¹ See Traynor, “Anonymity and the Internet”, 754 Practising Law Institute / Patents etc. Handbook Series 993 at 998 (2003).

⁴² 185 F.R.D. 573 (N.D. Cal. 1999).

⁴³ 140 F. Supp. 2d. 1088 (2001).

⁴⁴ [2004] F.C. 488.