Don't I know you? – Anonymity on the Net

Rick Shera Ll.B, MComLaw (Hons)
Partner, Lowndes Jordan
Vice-President, InternetNZ

Abstract

Nowhere do individual freedoms of association and speech vs the abuse of those freedoms (and the ability to stop the abusers) come into sharper focus than in the debate surrounding a right to anonymity (or pseudonymity) on the internet. Should those who send email or post information on the internet be required to say who they are? Or should they be entitled to be and remain anonymous even in the face of prosecution? Conversely, should we, and our children in particular, be able to avail ourselves of an express right to remain anonymous? These issues are being hotly debated worldwide. In this paper, the author briefly reviews some of those overseas developments and looks at how the issues might be dealt with under New Zealand privacy laws.

1. Introduction

1.1 …*Few would disagree that the World Wide Web offers unparalleled educational and recreational opportunities for our young people, but there are back alleys and dark corners of the Internet where our children can be exposed to inappropriate material or even become susceptible to offenders who view them as sexual objects. These offenders leverage the technology and anonymity of the Internet to trade and produce child pornography, explore their sexual interest in children, and to identify youth susceptible to manipulation and exploitation.*[1]

1.2 *The ubiquity of telecommunications, and the convergence of various technologies with telecommunications as the link, means that individuals are increasingly leaving minute by minute data trails that represent their communications, transactions and movements. This will increase in the coming years and many overseas experts see a right to anonymity (or pseudonymity) as critical to enabling individuals to retain some control over their personal information*[2]

1.3 The use of anonymity might be argued to be the ultimate expression of a right to privacy. The above quotes highlight the tension between anonymity as a privacy right and its use to purposefully hide identity in order to engage in anti-social or criminal behaviour.[3]

2. Identified, pseudonymous, anonymous

2.1 To see how this tension is or might dealt with, it might be helpful to first note that identification is not necessarily an all or nothing choice. At one end of

the scale there is what we can refer to as **identified contact** where the email, webpage or other data can easily be identified as originating from a particular person.

2.2 At the other end we have the types of contact where there is complete anonymity – **anonymous contact**. Even with a court order, the identity of the alleged originator would not be able to be revealed since no record of it ever existed. For, example commercial provider of anonymous internet services *Anonymizer.com* states on its site:

> *Anonymizer.com has been the leader in stemming the tide of online privacy invasion since 1996….The Anonymizer provides services which allow the anonymous use of Internet resources such as email, usenet, and the web. Because our business is privacy and anonymity, we do not require that users provide any personally identifiable information to use our services.*[4]

2.3 Between these two extremes there is however an option which might go some way to addressing the tension referred to above. That is where a person using a pseudonym makes the contact. The pseudonym has been allocated to that person by a third party who retains sufficient information to relate the pseudonym to the person in question – **pseudonymous contact**. Release of the information necessary to identify the pseudonym with his or her real identity is almost always resisted by the third party unless subjected to a court order. Even the obtaining of court orders to reveal the information can be difficult, as we shall see later in this paper.

3. Legitimate reasons for concealing identity

3.1 It is also important at this stage (and in the context of the often emotive topic of internet safety for children) to highlight the fact that anonymity or pseudonymity is not just the recourse of those "with something [sinister] to hide". There are many and varied reasons why someone might want to conceal their identity. The right to do so has been implicitly recognised in the *United Nations Universal Declaration of Human Rights*, which states:

> *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.*[5] *… Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.*[6]

3.2 In one of the leading US cases, America Online, Inc., one of the world's largest connectors of people to the internet, argued in its *amicus brief*:

The extensive use of screen names and other online pseudonyms is critical to the development of the Internet as a vehicle for individual expression. Users may wish to speak anonymously online for a variety of reasons: to criticize the activities of public officials or corporations without fear of retaliation, to "blow the whistle" on an employer who is engaging in unlawful or otherwise improper activity, to voice unpopular opinions on topical issues, to avoid harassment or even stalking by other online users, or to obtain advice or counseling on difficult problems or medical conditions. See, e.g., ACLU v. Reno, 929 F. Supp. 824, 849(E.D. Pa. 1996) ("Anonymity is important to Internet users who seek to access sensitive information . . . ."), aff'd, 521 U.S. 844 (1997). As one commentator has explained, anonymity not only allows speakers to experiment with unconventional or unpopular ideas without fear of ridicule or retaliation, but also "promises to make public debate in cyberspace less hierarchical and discriminatory than real world debate to the extent that it disguises status indicators such as race, class, gender, ethnicity and age which allow elite speakers to dominate real-world discourse." Silencing John Doe, 49 Duke L.J. at 896.[7]

3.3 To that list we can add another reason which is relevant to netsafety – the ability to interact anonymously/pseudonymously can be used to protect children. If a child is able to interact with others anonymously or behind the safety of a pseudonym then there must be less chance of persons that they come into contact with associating their online presence with the real world presence – with the potential physical peril that that can bring. Perhaps this mechanism might be a useful one for educators in netsafety to consider if they have not already done so.

3.4 Indeed, it is not too difficult to imagine the internet being populated with pseudo identities to such an extent that the distinctions between pseudonymous contact and identified contact might become meaningless.[8]

3.5 Of course the very pseudonymity that could assist in limiting the amount of personal information that children make available when they go online will also assist a potential predator in hiding not only their age but also possibly their sex.[9]

4. Uncovering true identity

4.1 Herein then lies the difficulty for law enforcement agencies in particular in their pursuit of criminal activity such as child pornography.

4.2 Clearly if the contact which is being investigated is truly an anonymous contact then resort will have to be made to more traditional forms of investigation. No details will be available to directly link the online persona to the real person

4.3 However, if the contact is pseudonymous (ie the third party provider has retained details of the pseudonym's real identity), then the next step will be to obtain these. In the US in particular this has caused some difficulty since the right to privacy is a First Amendment constitutional one, not easily brushed aside.

4.4 It would appear that the position which has been reached in civil cases at least is that a complainant wishing to obtain details from the third party against the wishes of the person using the pseudonym will need to first show a strong prima facie case in respect of the alleged wrongdoing and have tried to notify the defendant first.[10]

5. Australasia

5.1 In Australia, which, like New Zealand, does not have a constitutional guarantee of free speech/privacy, the Privacy Act 1988 (as amended in 2001) introduced a specific right of anonymity. Therefore:

> *Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.*[11]

5.2 It is suggested that New Zealand should adopt a similar right in relation to telecommunications and to that end the Privacy Commissioner has published for consultation a the draft Telecommunications Information Privacy Code 2002.[12]

5.3 In terms of the scale referred to above this will therefore mean that users of the internet who gain access through a New Zealand internet service provider will be able to do so completely anonymously.

5.4 Further, traffic information which might identify the originator of the data will be required to be deleted on termination of the call unless needed for billing purposes.[13] Therefore, it would seem that there would be little or no information to link an online presence to the real person where that person avails themselves of the rights in the draft code.

5.5 Granting an absolute an irretrievable right of anonymity might be argued to be swinging the balance too far in favour of privacy rights. The danger of doing so in terms of netsafety must be of concern.

6. Conclusion

6.1 It is always likely to be difficult to achieve a balance between the protection of children online and general privacy rights. Pseudonymity where anonymity is accorded until a court determines otherwise and orders identifying information released appears to strike some sort of balance.

6.2 The concern must be that in moving to a telecommunications right of complete anonymity reinforced by mandated removal of call data, this balance may be upset in New Zealand.

---

[1] Transcript of US Department of Justice "Operation Avalanche" child Porn announcement made by US Attorney General John Ashcroft, August 2001 <http://politechbot.com/p-02367.html>. Operation Avalanche involved the investigation and arrest of 100 individuals across the US connected with a child pornography enterprise, which, according to the report, had revenue in one month alone in excess of US$1 million.

[2] Consultation on Proposed Telecommunications Information Privacy Code 2002 – Information Paper, December 2001, *Office of the NZ Privacy Commissioner,* <http://www.privacy.org.nz/comply/tipcp.html> at p2.

[3] It should be noted that the problems of anonymity on the net extend further than just criminal behaviour. Other challenging areas where this problem arise for example, are enforcement action against copyright infringers and in respect to domain name cybersquatters.

[4] The Anonymizer, *Anonymizer.com*, < http://www.anonymizer.com/docs/privacy_statement.shtml>.

[5] Universal Declaration of Human Rights, 10 Dec 1948, Art 12 <http://www.unhchr.ch/udhr/lang/eng.htm>

[6] *Ibid*, Article 19.

[7] Brief Amicus Curiae of America Online, Inc. in *Joan Melvin v. John Doe et al*, Superior Court of Pennsylvania – Pittsburgh District, 24 February 2001 <http://legal.web.aol.com/decisions/dlpriv/melvinamicus%20.pdf>

[8] One can only sympathise with science fiction writers such as Tad Williams whose work of fiction (*Otherland*, 1996-2001) created a world where virtual reality pseudo identities are the norm – what was fiction as recently as 1996 now appears not only possible but necessary.

[9] Note that *The Net Generation: Internet Safety Issues for Young New Zealanders* published by The Internet Safety Group on 4 February 2002 indicates a suspicion amongst some respondents that they were given incorrect gender details by people they came in contact with online.

[10] *Dendrite International Inc. v. John Doe No 3* No. MRS C-129-00 (N.J. Super. Ct. Div 23 Nov 2000). For comment see Techlaw Journal Daily E-mail Alert, 12 July 2001, Alert No 225 <http://www.techlawjournal.com/alert/2001/07/12.asp> at p1; Mary P Gallagher *New Jersey Court Erects Roadblocks to flagging cyberspammers*, 18 July 2001, <http://www.law.com>

[11] Privacy Act 1988, National Privacy Principle 8.

[12] <www.privacy.org.nz/comply/tipc.html>. Consultation on this is open until 22 March 2002.

[13] Proposed Telecommunications Information Privacy Code 2002, Rule 9.