



PennState
Dickinson Law

DICKINSON LAW REVIEW
PUBLISHED SINCE 1897

Volume 110
Issue 3 *Dickinson Law Review - Volume 110,*
2005-2006

1-1-2006

On-Line Anonymity, Deindividuation and Freedom of Expression and Privacy

Follow this and additional works at: <https://ideas.dickinsonlaw.psu.edu/dlra>

Recommended Citation

On-Line Anonymity, Deindividuation and Freedom of Expression and Privacy, 110 DICK. L. REV. (2006).
Available at: <https://ideas.dickinsonlaw.psu.edu/dlra/vol110/iss3/10>

This Article is brought to you for free and open access by the Law Reviews at Dickinson Law IDEAS. It has been accepted for inclusion in Dickinson Law Review by an authorized editor of Dickinson Law IDEAS. For more information, please contact lja10@psu.edu.

On-Line Anonymity, Deindividuation and Freedom of Expression and Privacy

Katherine S. Williams*

I. Introduction

Life brings with it opportunities and risks, as do freedoms, rights and most major advances in civilization and technology. Each is both a blessing and a curse. In all cases it is essential to ascertain the essence of the positive aspect and protect it, knowing that this will always permit some negative or risky elements to survive. So it is with the Internet. In order to preserve the Internet's enormous potential to deliver freedom of expression, it is necessary to accept, or decide how to deal with, the potential harms that arise. The difficulty is always determining where, how and why to draw the line that curtails some expression, or some other right, by criminalizing activities or by blocking or otherwise preventing certain types of speech. This paper discusses one issue, anonymity on the net, and considers why it is so attractive and yet so potentially risky. Whilst mention will be made of legal and human rights elements, the focus is on the sociological and psychological attractions of anonymity. Issues to be addressed include whether anonymity causes unacceptable behaviours; why some use anonymity to gain an advantage, often an unacceptable advantage; and what this might mean for control of the net or other social or legal interventions.

II. Rights and Dangers Associated with On-line Anonymity

Those concerned with human rights and civil liberties consider anonymity on the web to be an important tool in guaranteeing freedom of expression. Anonymity permits individuals to profess their interests, beliefs and political ideologies without fear of reprisals from the state or any other powerful organisation. It also permits others to receive these views, an important aspect of many Human Rights instruments. For

* Lecturer in Criminology, Department of Law, University of Wales, Aberystwyth.

example, Article 10 of the European Convention on Human Rights and Fundamental Freedoms (ECHR) provides:

Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.¹

The right set out in the ECHR not only protects ones ability to impart and receive expression but also protects an international or cross-border dimension for those activities. Interference with anonymity would affect each of these aspects of the right. Furthermore, at its first opportunity, the European Court of Human Rights (ECtHR) declared that freedom of expression covers unpopular as well as popular ideas:

Freedom of expression . . . is applicable not only to "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population. Such are the demands of pluralism, tolerance and broadmindedness without which there is no "democratic society."²

Clearly, it would be a gross violation of the right of expression to curtail or otherwise interfere with the use of anonymity without a sound reason for the interference.

As well as protecting freedom of expression, anonymity also protects the privacy of the individual by preserving his/her identity, as guaranteed in Article 8(1) of the ECHR³ which refers to respect for private and family life. The Court has adopted a broad interpretation of private and family life to include not only the notion of the "inner circle," but also "to a certain degree the right to establish and develop relationships with human beings."⁴ Establishing and developing relationships must include the boundaries of those relationships, thus permitting privacy and anonymity. Interestingly, due to the impersonal nature of contact on the Internet, all of the normal safeguards as to whom one is dealing with are absent. In the real world, if I meet someone in person, I can form my own assessment of many of that person's traits, however erroneous or prejudiced that may be. In the virtual world, this

1. European Convention on Human Rights and Fundamental Freedoms, Nov. 4, 1950, art. 10, Europ. T.S. No. 5 [hereinafter ECHR].

2. *Handyside v. United Kingdom*, 24 Eur. Ct. H.R. (ser. A) at 754-55 (1976).

3. ECHR, *supra* note 1, art. 8. "Everyone has the right to respect for his private and family life, his home and his correspondence." *Id.*

4. *Niemetz v. Germany*, App. No. 251-B, 16 Eur. H.R. Rep. 97 (1992).

is not possible, and individuals are free to alter their sex, age, race, religion, status, etc.—in effect re-inventing themselves, physically, psychologically and socially. They can invent numerous personae for use in different situations or to give them different possibilities in the same sector of the net. Their new personae may help them to become empowered in a way that they feel is not possible in the real world. Fantasy, games, whistle blowing, and the provision and enjoyment of counselling or help and advice on the net, especially in areas such as mental health which is so stigmatised in the community, may all be enhanced by anonymity and may in turn enhance the lives of the users and possibly also of others. Anonymity therefore serves two important rights.

Unfortunately, anonymity also brings great risks—it facilitates the commission of crimes, torts and other harmful, anti-social or deviant activities with impunity. Individuals can libel others, damage companies, damage economies, destabilise regimes, disseminate hate speech, prey on children or other vulnerable individuals, and disseminate criminal or offensive information or images. Governments fear the possibility of individuals being strongly persuaded politically by information in the virtual community. This fear is heightened because the World Wide Web can also provide the information necessary to subvert the state or to conduct terrorism, such as political information or propaganda and bomb making instructions, thus providing both the ideology and practical information necessary to destabilise a regime. Governments prefer to have some control on information. Particularly in our information era, political power and authority is heavily interwoven with the dissemination of information (or the control of its dissemination). This interweaving of power and information or knowledge is not new and was the reason for the early control of the printing press through licensing⁵ and the use of seditious libel. Anonymity for those disseminating information to a mass audience is therefore always of concern.

Interestingly, as well as these often-discussed polarised possibilities, anonymity on the Internet has other potentially positive effects and great positive potential. In some circumstances, anonymity helps to protect against certain risks. For example, one of the greatest protections from predators on the net is anonymity because it allows children and other vulnerable individuals to remain anonymous, particularly in on-line chat rooms. Children need to be educated about the reasons for protecting their anonymity and the dangers inherent in failure to do so. Children

5. See S.J. Lewis, *An Instrument of the New Constitution: The Origins of the General Warrant*, 7 J. LEGAL HIST. 256-72 (1986).

should be advised to protect their identities and their personal information in on-line chat rooms in case those they are chatting with are very different from the personae they project on-line.⁶ This protection can be enhanced by use of encryption, anonymous remailers and other privacy devises. However, the most dangerous aspect of chat rooms is the fact that children often choose to reveal their identities and locations to those they feel they can trust, usually someone they feel they have "got to know" in the chat room. According to the Cyberspace Research Unit, one in ten young chat users will attend a face-to-face meeting with another chat user, and three quarters of these will not take an adult.⁷ The Research Unit also found young users did not understand how, when or why to retain anonymity or how to protect themselves in the environment. Neither schools nor parents were doing enough to educate children about this medium or about other new communications media.⁸ If anonymity is attacked, criminalised or portrayed as unacceptable, this situation is likely to get far worse because the law abiding will obey whilst those intent on criminal behaviour will continue to abuse anonymity.

There are strong positive reasons to support anonymity in the cyber world, which include protecting the rights to freedom of expression and privacy and protecting the vulnerable. As suggested by Rowland,⁹ there is a need for a clear risk assessment concerning the use and abuse of anonymity on the net to ascertain how great a problem it really represents and whether the benefits outweigh the drawbacks.

This piece does not purport to fill this gap in research but does assess whether anonymity is really the problem. It also questions whether anonymity causes people to transgress on the net or merely frees them as in other non-computer based situations and asks why this activity has not proven to be as prevalent or problematic as was expected.

6. CYBERSPACE RESEARCH UNIT, YOUNG PEOPLES USE OF CHAT ROOMS: IMPLICATIONS FOR POLICY STRATEGIES AND PROGRAMS OF EDUCATION (2002), <http://www.uclan.ac.uk/facs/science/psychol/Homeoff2.pdf>.

7. *Id.* at 4.

8. *Id.* at 2-5.

9. Diane Rowland, *Anonymity, Privacy and Cyberspace*, BRITISH & IRISH LAW, EDUC. AND TECH. ASS'N CONFERENCE: ELEC. DATASETS AND ACCESS TO LEGAL INFO. (2000), <http://www.bileta.ac.uk/pages/Conference%20Papers.aspx> [hereinafter Rowland, *Anonymity*]. See also Diane Rowland, *Privacy, Freedom of Expression and CyberSLAPPs: Fostering Anonymity on the Internet?*, BRITISH & IRISH LAW, EDUC. AND TECH. ASS'N CONFERENCE: INFO. IN THE ONLINE ENV'T (2003), <http://www.bileta.ac.uk/pages/Conference%20Papers.aspx> [hereinafter Rowland, *Privacy*].

III. Deindividuation and Anonymity

It has been suggested that work on deindividuation¹⁰ might explain the link between anonymity and unacceptable or anti-social activities on-line. Deindividuation is a social psychological theory; its origins concerned the behaviour of individuals in crowds. It sought to explain the transformation of an apparently rational and responsible individual into an unruly and irresponsible person. The essence of the theory is that inner restraints are lost when people are no longer seen or considered as individuals.¹¹ The early defining aspects of the phenomenon, and the ones which people intuitively feel will release individuals to offend on the net, are that an individual: (1) joins a group or crowd; (2) enjoys a sense of being submerged or subsumed and anonymous; (3) suffers from a loss of self-awareness;¹² and (4) feels a diffuse responsibility and is thereby more open to suggestions. In the early theory as set out by Le Bon,¹³ these suggestions came from the group, and the individual was on a moral or ethical holiday during which the morals of the mass or group could be substituted for those generally used or enjoyed by the individual—basically, the individual is not him/herself whilst in the group.¹⁴ Instead, he or she is part of a larger and different whole, a puppet of the group or its leader. The ability of the individual to regulate his/her own behaviour is weakened, as is the ability to conduct rational and long-term planning. There is therefore a tendency to react to situations quickly without considering all the consequences and to give little thought to the way others might view the behaviour, all of which tends to give rise to impulsive and unrestrained behaviour. This theory has been used to explain various collective behaviours, like violent crowds and lynch mobs, and has also been linked to other criminal and deviant¹⁵ activities such as stealing, violence and aggressive driving.¹⁶ Although early links were to the group, many modern theorists have

10. GUSTAVE LE BON, *THE CROWD: A STUDY OF THE POPULAR MIND* (Transaction Publishers 1995) (1895).

11. L. Festinger et al., *Some Consequences of Deindividuation in a Group*, 47 *J. ABNORMAL & SOC. PSYCHOL.* 382-390 (1952).

12. Phillip G. Zimbardo, *The Human Choice: Individuation, Reason, and Order Versus Deindividuation, Impulse, and Chaos*, 17 *NEB. SYMP. ON MOTIVATION* 237 (W.T. Arnold & D. Levine eds., Univ. of Neb. Press 1969).

13. LE BON, *supra* note 10.

14. This would explain the classic Stanford Prison Experiment. For more information, see Philip G. Zimbardo, *Stanford Prison Experiment: A Simulation Study of the Psychology of Imprisonment Conducted at Stanford University* (2005), <http://www.prisonexp.org/>.

15. See Diane Rowland, *Gripping, Bitching and Speaking your Mind: Defamation and Free Expression on the Internet*, 110 *PENN ST. L. REV.* 519 (2006).

16. P. Ellison et al., *Anonymity and Aggressive Driving Behaviour: A Field Study*, 10 *J. SOC. BEHAV. & PERSONALITY* 256 (1995).

linked deindividuation to anonymity—those who believe that their identity is unknown will behave in this same impulsive and unrestrained manner.¹⁷ Ellison et al.¹⁸ linked the anonymity of drivers to their behaviour behind the wheel; Zimbardo¹⁹ showed that people were more likely to administer a stronger electric shock when they were hooded and therefore unknown.

Deindividuation has also been associated with other phenomena such as genocide and with disinhibition in other settings such as computer mediated communication. To assess its utility as an explanation in the last area, it is necessary to analyse the recent explanations for deindividuation which have moved away from reliance solely, or even largely, on anonymity towards contextual factors such as reduction of responsibility, arousal, sensory overload, a lack of contextual structure or predictability and even the effects of various substances.²⁰ The connection of deindividuation to these different contextual factors was not the only change to the theory. The need for the physical presence of the group or crowd was also dispensed with so that loss of individuality might result in other contexts and could itself lead to a loss of control. This means that moral restraints would no longer hold the individual, allowing him or her to participate in impulsive, emotional, irrational, regressive and intense behaviour some of which is likely to be unacceptable to others. The part played by anonymity is currently thought to be substantially reduced, and the link now is with reduced self-awareness which decreases the possibility of self-regulation, thus giving rise to the anti-normative and disinhibited behaviours traditionally linked to deindividuation. However, the links between deindividuation and this negative behaviour have not been born out in empirical studies. Even Zimbardo²¹ noted that his findings were not predictable or always supportive of the theory, and in a meta-analysis of sixty tests of the theory, Postmes and Spears²² found insufficient support for it.

In this environment there has been a further shift in the theory to what is called the Social Identity Theory of Deindividuation (SIDE).²³

17. See, e.g., *id.*; Tom Postmes & Russell Spears, *Deindividuation and Antinormative Behaviour: A Meta-Analysis*, 123 PSYCH. BULL. 238 (1998); Zimbardo, *supra* note 12.

18. Ellison, *supra* note 16.

19. Zimbardo, *supra* note 12.

20. *Id.*

21. *Id.*

22. Postmes & Spears, *supra* note 17.

23. Stephen D. Reicher, *Crowd Behaviour as Social Action*, in JOHN C. TURNER ET AL., REDISCOVERING THE SOCIAL GROUP: A SELF-CATEGORIZATION THEORY (Oxford Blackwell 1987). See also Stephen Reicher et al., *A Social Identity Model of*

Within this theory, anonymity has been considered too simple a frame of reference. Instead, the self is considered to be a complex construct consisting of at least two subsystems: (1) personal identity—the qualities that make an individual who he or she is and how he or she is different from others; and (2) social identity or identities—the groups the individual belongs to and the identity which comes to the fore when the individual is in a particular group. SIDE links deindividuation not with anti-normative or unruly behaviour but rather with a shift from individual towards group or social frames of reference and norms which are shared by others. These frames of reference may be anti- or pro-normative, depending on the group ethics. This still means that behaviour is dominated by external cues, rather than internal standards, but respects that often those cues are more controlled than the individual might be and may vary depending on the group and its normative structures or expectations. This still retains the essence of the theory as behaviour which occurs without, or with reduced dependence on, internal or wider social references. The theory is also still linked to anonymity as the effects of movement from internal to social or group frames of reference are more likely to occur and to be more marked depending upon the presence or absence of anonymity.

IV. Is Anonymity Linked either Causally or Otherwise to Unacceptable Behaviour on the Net?

In early associations of deindividuation with computers, the argument went that whilst using computers many felt anonymous—they were not physically overlooked and viewed their virtual world as separate from their real world. This meant that whilst on the computer people did not feel constrained by either normal internal or social inhibitors. They were morally and ethically liberated to behave as they chose.²⁴ Many argued that this meant that computer users would transgress normal boundaries on a regular basis and that normally law-abiding, caring and moral individuals would be liberated from their internal morals or ethics and would begin to behave badly, rudely, insensitively and maybe even criminally. Within this early work it is often unclear whether the unacceptable or harmful behaviours were linked to groups, to anonymity, to the medium of communication (a computer), to the effect of not communicating directly with a real person which removes the need to take their feelings into consideration and can result in a failure to think of the other person as human, to an absorption

Deindividuation Phenomena, 6 EUR. REV. SOC. PSYCHOL. 161 (1995).

24. Jonathan Siegel et al., *Group Processes in Computer-Mediated Communication*, 37 ORGANISATIONAL BEHAV. AND HUM. DECISION PROCESSES 157 (1986).

with or a type of addiction to the media and a resulting inability to consider other things, to a reduction of inhibitions more generally, or to some other factor. The question as to whether it was the medium (the computer) or some other facet which was linked to the behavioural changes was difficult to resolve. Some work²⁵ has suggested that both the computer-based medium and the anonymity can have a marked effect on behaviour, leading to less traditional behaviours. Cooper's²⁶ study analysed individuals in a brainstorming session. The research concluded that the link was with more controversial, though often useful, solutions in a brainstorming session. Some of these solutions were so offensive as to cause others in the brainstorming session to withdraw. However, when tested, results generally have not shown such a marked effect. They have not backed up general deindividuation theory as an explanation for on-line transgressions.²⁷ This is less surprising when one considers that the researchers did not take account of SIDE.

As mentioned above, recently the SIDE model of deindividuation has become more influential as the explanation of how groups affect behaviour. This model has been applied to computer-mediated communication and has uncovered more consistent support for deindividuation as espoused in SIDE. Therefore, behaviours mediated by the group or social self rather than the private self come to the fore in these on-line group discussions. Where the group tends toward damaging or generally unacceptable behaviours, these are replicated by members of the on-line group,²⁸ but where the group dynamics tend towards polite or other ethical behaviours, these behaviours are just as likely to be replicated by group members. In these pieces of research, the effects of anonymity were found to depend on a number of factors such as the salience of the group membership to the individual and to the group and the social context of the interaction. So, anonymity and, in particular, dissociation with the physical attributes of other members (not

25. William H. Cooper et al., *Some Liberating Effects of Anonymous Electronic Brainstorming*, 29 RES. 147 (1998).

26. *Id.*

27. Joseph S. Valacich et al., *Group Size and Anonymity Effects on Computer-Mediated Idea Generation*, 23 SMALL GROUP RES. 49 (1992). See also K.E. Greenwood, *Deindividuation v. Individuation on the Computer*, 27 INT'L J. OF PSYCHOL. 305 (1992).

28. Karen M. Douglas & Craig McGarty, *Identifiability and Self-Presentation: Computer-Mediated Communication and Intergroup Interaction*, 40 BRIT. J. OF SOC. PSYCHOL. 399 (2001). See also Russell Spears & Martin Lea, *Social Influence and the Influence of the 'Social' in Computer-Mediated Communication*, in CONTEXTS OF COMPUTER-MEDIATED COMMUNICATION (Martin Lea ed., 1992); Karen M. Douglas & Craig McGarty, *Internet Identifiability and Beyond: A Model of the Effects of Identifiability on Communicative Behaviour*, 6 GROUP DYNAMICS 17 (2002); Martin Lea & Russell Spears, *Computer-Mediated Communication, Deindividuation and Group Decision-Making*, 34 INT'L J. OF MAN-MACHINE STUD. 283 (1991).

being able to “see” them) does not necessarily lead to bad behaviour unless that behaviour is encouraged by the group or is part of its being. Groups with pro-social norms can increase the tendency for people to act in accordance with those positive social norms. The power, influence and limits of the group over norms of behaviour was illustrated by Postmes et al.,²⁹ who discovered that in-group communication (both content and form) was governed by group norms. Adherence to these group norms increased over time as the individual became socialised into that group, but these group norms were limited to the boundaries of the group, and therefore communication outside the group was governed by other social norms. Furthermore, the group effects were found to be amplified in a depersonalised or anonymous environment, where group members were not known to each other, or were only known by pseudonyms.³⁰ Although the effects of the medium and anonymity may also be heavily affected by national culture/identity, the effects of each, and the way in which they interact, need to be further studied.³¹

Another aspect of deindividuation theory which is of interest is that of Reicher’s recent work³² showing that the effects of deindividuation are strongest when the in-group are visible to one another. This may suggest anonymity reduces the effects of deindividuation; however, the increased effect of in-group visibility was equally strong even when the visibility that people believed they had was with an invented persona. Barrero and Ellemers³³ found interesting results when they studied anonymity within the group. They found that deindividuation measured by the willingness of the individual to conform to and work for the group was strongest when the individuals were either totally anonymous or totally visible to the in-group. Between these extreme states group effects were lower. Reicher et al.³⁴ also found that generally the effects of SIDE are strengthened where the group has to overcome out-group repression in order to express its defining nature. The effects of repression and internal cohesion emphasise the group frames of reference. Therefore,

29. Tom Postmes et al., *The Formation of group norms in computer-mediated communication*, 26 HUMAN COMM. RES. 341 (2000).

30. Tom Postmes et al., *Intergroup Differentiation in Computer-Mediated Communication: Effects of Depersonalization*, 6 GROUP DYNAMICS 3 (2002).

31. Bruce A. Reing & Roberto J. Mejias, *The Effects of National Culture and Anonymity on Flaming and Criticalness in GSS-Supported Discussions*, 35 SMALL GROUP RES. 698 (2004).

32. S. Reicher et al., *More on Deindividuation, Power Relations Between Groups and the Expression of Social Identity: Three Studies on the Effects of Visibility to the In-Group*, 37 BRIT. J. SOC. PSYCHOL. 15 (1998).

33. Manuela Barrero & Naomi Ellemers, *The Impact of Anonymity and Group Identification on Progroup Behavior in Computer-Mediated Groups*, 33 SMALL GROUP RES. 590 (2002).

34. Reicher, *supra* note 32.

behaviours consistent with these rather than with personal internal or wider social controls are likely to arise.³⁵ This has been at least partially replicated in the on-line world where the need to resist a powerful out-group intensified the capacity for resistance.³⁶ For our purposes, the work by Spears et al. is even more revealing.³⁷ They argue that computer communication is not substantially different from face-to-face communication. In fact they claim that in group situations such as chat rooms, newsgroups etc., the impetus to conform may be stronger than in face-to-face interactions.

The effects of aspects like anonymity and deindividuation in the on-line environment must never be exaggerated. Though when using SIDE both anonymity and computers seem to have an effect, this effect is unlikely to be greater than it would be for similar media under similar conditions. Hobman³⁸ suggests that the immediate effects in the on-line environment may be amplified and greater than those in other environments (face-to-face) but that these differences ironed themselves out very quickly, over a few days.

All in all, neither anonymity nor the on-line environment (nor their combination) *per se* can be said to cause unacceptable or criminal behaviours any more than is the case in the real world. Clearly, however, anonymity is sensibly and rationally chosen by those who decide to perform negative activities, whether criminal or other, and who do not wish to be held to account for those activities. Therefore, although anonymity is likely to be used in terrorist cells or in child pornography rings, it does not cause people to become involved in such activities. In these settings the anonymity and reduced self-awareness which give rise to deindividuation may be connected with the activity. For example, they possibly facilitate the activity and clearly render it easier to take part in the activity with impunity by making detection more difficult. However, and crucially, these aspects are not causative; neither anonymity nor even deindividuation itself explains the causes of computer-related criminality or other harmful uses of computing.

35. *Id.* See also S. Reicher & R. M. Levine, *Deindividuation, Power Relations Between Groups and the Expression of Social Identity: The Effects of Visibility to the Out-group*, 33 BRIT. J. SOC. PSYCHOL. 145 (1994); S. Reicher & R. M. Levine, *On the Consequences of Deindividuation Manipulations for the strategic Communication of Self: Identifiability and the Presentation of Social Identity*, 24 EUR. J. SOC. PSYCHOL. 511-524 (1994).

36. Russell Spears, et al., *Computer-mediated Communication as a Channel for Social Resistance: The Strategic Side of SIDE*, 33 SMALL GROUP RES. 555 (2002).

37. Russell Spears, et al., *When are the Net Effects Gross Products? The Power of Influence and the Influence of Power in Computer-Mediated Communication*, 55 J SOC. ISS. 91 (2002).

38. Elizabeth V. Hobman et al., *The Expression of Conflict in Computer-Mediated and Face-to-Face Groups*, 33 SMALL GROUP RES. 439 (2002).

Anonymity and deindividuation provide no magic solution concerning why these activities arise, although they do help to explain how individuals become more and more drawn into the group mores and how these can overcome either individual norms of behaviour or wider social mores. This effect is linked not to anonymity but to deindividuation, especially as espoused through SIDE, and therefore is related to the complex interaction of personal identity with social identity or identities in an on-line environment. It is the power of the group that has the effect not the anonymity. Therefore, although intuitively we may think that anonymity causes the bad behaviour, this is not the case. The most anonymity may be doing is impeding detection and thereby allowing people to choose negative activities. In this situation controlling anonymity would only reduce the amount of criminal or unacceptable behaviour on-line to the extent to which it facilitated, or was believed to facilitate, detection. It is perfectly possible that individuals commit negative activities believing they will go un-punished. This may happen with or without anonymity. To control criminal activities on the net, it is necessary to search elsewhere for causative explanations of the behaviour and/or to increase detection rates. We must consider whether the potential increase in detection rates is enough to warrant interference with on-line anonymity.

V. Is Control of or Curtailing of Anonymity Compatible with Protection of Human Rights?

Under the ECHR both freedom of expression (Article 10) and privacy (Article 8) are limited in specific instances. The second paragraph of each of these articles permits interference by a public authority with the rights set out in the first paragraphs.³⁹ Article 8(2) defines the circumstances in which the rights may be interfered with as follows:

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.⁴⁰

Article 10(2) defines the circumstances in which the rights may be interfered with as follows:

The exercise of these freedoms, since it carries with it duties and

39. See *supra* note 1 for article 10(1) and *supra* note 3 for article 8(1).

40. ECHR, *supra* note 1, art. 8.

responsibilities, may be subject to such formalities, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority of the judiciary.⁴¹

In brief each right may be interfered with if:

- i. interference is in accordance with the law, as clearly set out in statute or case law;
- ii. the restriction serves one of the legitimate aims set out in the second paragraph's exhaustive list, and;
- iii. the interference is necessary in a democratic society.

Only exceptions set out in the second paragraph of each article will be accepted as legitimate reasons to interfere with that right. Each list is exhaustive and is to be narrowly construed so that states cannot extend interpretation of the provisions beyond their ordinary language.

If controls on, or restrictions of, anonymity were set out in statute law, the first element would be met. In each case most of the dangers often associated with anonymity on-line would be covered, or appear to be covered, by the permitted aims set out in each of the second paragraphs. For example, states might claim that restrictions on anonymity would serve the interests of national security (or, in the case of Article 10, territorial integrity), the prevention of disorder or crime, or, in the case of expression under Article 10, the protection of the reputation or rights of others. The real issue concerns the third prong of the test justifying interference with a right, which asks whether that interference would be necessary in a democratic society. For a restriction to be necessary, it should be directed to meeting a "pressing social need," and it should be proportionate to that need.⁴² Proportionality is assessed by asking whether the interference with the right is more extensive than is justified by the legitimate aim. The balance, therefore, is between the extent and nature of the interference and the reasons that justify it, rather than directly between the interference and the right. Wherever possible, the state must achieve the legitimate aim by the least intrusive means. The court (ECHR) takes

41. ECHR, *supra* note 1, art. 10.

42. See *Sunday Times v. United Kingdom*, 30 Eur. Ct. H.R. (ser. A) (1979) (Thalidomide case); *Handyside v. United Kingdom*, 24 Eur. Ct. H.R. (ser. A) at 754-55 (1976).

account of factors such as whether the right is sufficiently important to warrant the requirement of a particularly strong reason for any interference and whether the interference is so drastic that it deprives the right-holder of the very essence of the right. Importantly, the court also inquires into whether the harm caused to the right-holder is potentially outweighed by any benefit which the interference might achieve through furthering the legitimate aim. The court permits the state a “margin of appreciation” in assessing both the existence of a pressing social need and the appropriate response which should be taken to deal with it. This leeway for discretionary judgment is permitted because it is thought that national authorities are in a better position than is an international tribunal to judge what is necessary within their own state. The discretion is limited and ultimately the European Court of Human Rights will decide whether there is a pressing social need and whether the limitation is proportional to that need. Therefore, the state has to be able to prove: that there is a need for any restriction; that the measures taken will meet that need; that the standards used by the local authorities conform with the ECHR; and that all of the state’s actions can legitimately be considered proportionate.

From this it is clear that it is important to take account of how great an interference there is with the interests being protected. Anonymity is used to allow individuals to express beliefs and political ideologies without fear of reprisals from states. To interfere with rights to anonymity would therefore severely impair individuals’ rights to freedom of expression in areas of important political and other belief. Interference with anonymity would also impede the ability of individuals to make known to others the persona by which they wish to be known or to limit the amount of information about themselves to which others on-line are permitted access. Each of these is an important interference with the right guaranteed under the ECHR. As control of, or limitation of, anonymity may interfere with the content of material expressed on-line, it goes to the very essence of the right and therefore requires strong justifications in order to interfere with it. The previous section suggested that there was no proven causal link between anonymity *per se* and the negative behaviours generally associated with computers. For this reason interference with anonymity would be unlikely to protect against harmful or criminal behaviours occurring on the net. The most interference would achieve would be facilitating law-enforcement officers in investigating and prosecuting any criminal transgressions and/or facilitating civil actions. Therefore, whilst there is a pressing social need both to prevent criminal activity being conducted on-line and to protect national security, the schism between anonymity and any causal link to criminality or unacceptable behaviour means that general

interference with rights to anonymity would be unlikely to reduce criminal activity or prevent any threats to national security. Instead, interference would prevent individuals from expressing themselves and their beliefs. The aim of prevention is legitimate and, if achievable, might justify control of anonymity. However, because the benefit which might be achieved through furthering the legitimate aim would be small and the harm to some right-holders would be great, blanket or general interference with anonymity would not be justified. The harm caused to the right-holder is not outweighed by any benefit which the interference might achieve through furthering the legitimate aim.

If interference with anonymity cannot be justified on the preventive grounds, is it possible to justify such measures in order to aid in the detection and prosecution of individuals who use the veil of anonymity to commit offences with impunity? Arguably this should not suffice, at least not to remove anonymity generally. However, as has been argued elsewhere,⁴³ it may be sufficient to lower the veil of anonymity in particular cases. Therefore, where a crime has been committed it may be justifiable to permit the authorities the power to access a key allowing them to look behind the anonymity, thus permitting them to prosecute or to prevent further breaches of criminal laws or of national security. In relation to this it is important to note that anonymity is increasingly an illusion. The level of anonymity that Internet users enjoy today is, due to technical changes, considerably lower than it used to be. It may be that what is necessary is to educate the public about the true situation, thus discouraging those who participate in anti-social behaviours because they believe that they are anonymous and therefore likely to escape detection.

The present work is not, however, conclusive. What is really necessary at this point is not only the risk assessment called for by Rowland⁴⁴ but also extensive research into the effects of anonymity and its links with harmful behaviours. Lawyers pay far too little attention to causative links or their absence as found in other disciplines. Where, as with restrictions on rights, there is a need to assess not only the use and abuse of particular activities but whether restrictions would deliver the claimed benefit, there is a need to consider carefully the presence or absence of causative links between the abuse and the element which may be restricted. Without this, restrictions of rights should not be permitted, as the claimed benefits used as justifications for them would not be

43. See, e.g., Akdeniz Yamen et al., *BigBrother.gov.uk: State Surveillance in the Age of Information and Rights*, 2001 CRIM. L. REV 73 (2001). See also, Katherine S. Williams, *Facilitating Safer Choices: Use of Warnings to Dissuade Viewing of Pornography on the Internet*, 15 CHILD ABUSE REV. (forthcoming 2006).

44. See Rowland, *Anonymity*, *supra* note 9. See also Rowland, *Privacy*, *supra* note 9.

proven. The case to protect anonymity, at least between users, is strengthened when one takes account of the fact that general removal of anonymity might actually increase the danger for some of the most vulnerable users of the world-wide-web.
