15th BILETA Conference: “ELECTRONIC DATASETS AND ACCESS TO LEGAL INFORMATION”.

Friday 14th April 2000.
University of Warwick, Coventry, England.

Anonymity, Privacy and Cyberspace

Diane Rowland
Department of LawUniversity of Wales, Aberystwyth, UK

Abstract

This paper examines some of the issues relating to the protection of privacy on-line, specifically whether anonymity is a necessary and proportionate response to the issues raised. The subject is considered in the light of the relationship between anonymity and privacy, the application of existing data protection law, current proposals and the possibility that increased anonymous use of the Internet and World Wide Web may, itself, create further regulatory challenges.

Keywords: privacy, anonymity, data protection, deindividuation

Introduction

The desire of individuals to control who knows what about them is not a new concern and neither is the collection and storage by individuals and organisations of personal information about others a new habit. Nonetheless technological advances, particularly in the second half of the twentieth and now into the twenty first century have brought a number of the issues concerning personal information sharply into focus and given new urgency to calls for a more consistent legal approach to privacy issues. In 1968, Fried commented in response to technological advances (specifically in relation to surveillance techniques) "(t)he more insidious intrusions of increasingly sophisticated scientific devices into previously untouched areas and the burgeoning claims of public and private agencies to personal information have created a new sense of urgency in defence of privacy."(Fried (1968 p. 475)) Some years later Gavison (1980 p. 465) observed that, although the requirement of privacy was not new, the increased concern with its loss was a recent development and that the "main reason for this modern concern appears to be a change in the nature and magnitude of threats to privacy, due at least in part to technological change ... advances in the technology of surveillance and the recording, storage and retrieval of information have made it either impossible or extremely costly for individuals to protect the same level of privacy they once enjoyed." That this sense of urgency in relation to the threat remains is exemplified by the latest report from the Electronic Privacy Information Center (EPIC) in December 1999 which concluded that "the current practices of the on-line industry provide little meaningful privacy protection for consumers ... on balance we think that consumers are more at risk today than they were in 1997 - the profiling is more extensive and the marketing techniques are more intrusive."(EPIC 1999)

The purpose of this paper is to review the nature of the threat to privacy and more specifically, in the light of recent reports and proposals, to examine whether the concept of privacy includes a right to be anonymous and the extent to which the perceived problems can be ameliorated by measures which allow users to retain anonymity. It must not be forgotten that measures which foster anonymity in order to protect privacy may, incidentally, facilitate or even encourage anti-social and illicit behaviour. This calls not so much for a balancing of rights perhaps as a balancing of the relative risk from different threats. There are also other interests which are fuelling the debate. Prior to about 1996, the prevailing commentary seemed to suggest that, on balance, allowing, not to mention favouring, anonymity had the propensity to turn Cyberspace into the ungovernable space prophesied in the popular press. The subsequent rapid expansion of e-commerce and therefore, the increasing presence on the Internet of large corporate actors together with the desire of individual Governments to promote this type of activity has tended to reverse the debate. The general perception seems to be that consumer protection issues, including privacy concerns, relating to commercial transactions over the Internet have eclipsed other threats. In the words of the EPIC report referred to above "(i)t appears that commercial activity on the Internet is driving the increased collection of personal data".

Privacy in Cyberspace

In the 1970s and 1980s, increasing computerisation was seen to pose a threat to the privacy of individuals because of the propensity of computers to store, link, manipulate and provide access to ever increasing quantities of personal data. Further, both data matching and personal profiling were facilitated by the ease of correlation of data held by different users and at different geographical locations. The nature of the threat has undergone a subtle change with the advent of global networks of computers which are now being used by a vast range of different actors; from the individual to the corporate, private and governmental organisations, education for a multitude of uses; educational, recreational, personal, commercial. Further the intentionally decentralised nature of this global network makes it difficult to gain any meaningful and accurate estimate of the total number of users, much less the relative proportions of the various types of use.

A particular feature is the change in characteristics of the average user - originally computers were the province of the specialist and technocrat but now they are the tool of the person on the Clapham omnibus who may or may not have any insight into the modus operandi of the technology. The average user may still not be aware of the traceability of operations performed during on-line activities. A number of common features such as the creation of `navigation trails', the existence of privileged websites, the use of `cookies' to capture and retain information about users and so on may effectively replicate other data matching processes (see Working Party 1999a). The common use of the World Wide Web as a vast information source raises the possibility of retaining and collating trace information from successive Web searches which could prove very useful for personal profiling purposes. In addition, it is possible that access/service providers may hold personal details about their clients, transactional information such as the types of site visited, connection times etc., and even, perhaps, the content of private communications such as e-mail (see Working Party 1998). As these aspects have become more widely known and appreciated, there has, in response, been a consequent increase in the development and use of `privacy enhancing technologies' such as encryption and anonymous remailers.

A further difficulty is that the standard geographical concepts of jurisdiction may become meaningless when applied to activities conducted on the Internet. This is exacerbated by the fact that there is not necessarily any consensus over the regulation of these activities in specific geographical jurisdictions. The Internet pioneers saw its development as a step towards a global collective information forum centred in ideals of free speech and empowerment of the individual. In some respects it exhibits these characteristics but in others the increased use for commercial purposes runs counter to this objective. Nonetheless the medium is still one which is, by and large, subject to less regulation than more traditional methods of communication. Indeed the District Judge Dalzell in *ACLU v Reno* (<http://www2.epic.org/cda/cda_dc_opinion.html>) was at pains to point out why the standards embodied in the regulation of broadcasting were not necessarily appropriate for regulation of the Internet, a fact which was later supported by the Supreme Court (136 L Ed 2d 436 and

<http://www2.epic.org/cda/cda_decision.html> A number of physical jurisdictions have tried to regulate communication on the Internet but any global response needs to take into account cross-cultural factors which may lead to the perceived freedom being viewed as either desirable or alternatively as unacceptable licence. Which of these views is taken will determine whether Internet regulation is seen as interference with freedom of expression or as the imposition of recognised or acceptable minimum standards.

This is not to say that the invisible collection and correlation of personal data represents the sole threat to privacy in Cyberspace. It might be thought that the concept of a personal space has little meaning within Cyberspace but it certainly seems to be the case that bombarding recipients with unwanted e-mails or `cyberstalking' may also be felt by the victim as an unwarranted intrusion on privacy. In the UK the Protection of Harassment Act 1997 has been used to deal this type of activity and there also seems no reason, in principle, why the decision of the Court of Appeal in *Khorasandjian v Bush* ([1993] QB 727) should not be used for unwanted and intrusive e-mails where these are received in the home.

The relationship between privacy and anonymity

Privacy is a topic which has been much explored in the academic literature (see e.g. Westin A.F. (1967) Wacks R (1989) and (1993)). There has been extensive and ongoing debate about the scope and components of the subject and about the precise nature of those individual components. A number of possible constituent elements of the right have been formulated. These can be said to begin with `right to be left alone' developed by American judges in the nineteenth century from English common law precedents and widely believed to have been given academic credence by Warren and Brandeis (1890), but also include more specific aspects such as a right to be control information about oneself and a right to a personal space, free of unwanted and unwarranted physical intrusion. Some of these definitions do little to assist an analysis of the role of the law and its effectiveness in dealing with the protection of privacy and specifically in providing remedies for its infringement as many depend on the subjective view and behaviour of the individual.

One reason why privacy seems to remain such an elusive concept is that what is expected and acceptable exhibits great variation. There is also a collective element, although this is susceptible to variation between different communities and social circles. Within any particular community individuals may be criticised if they `keep themselves to themselves' too much or, conversely, if they reveal all about themselves. Those in enclosed religious orders may experience a level of isolation from the rest of the world which some would equate with privacy but there may be little protection from intrusions of privacy by others in the same community. It could be said that the community has privacy but not the individual. Indeed, total privacy is both a practical impossibility, except perhaps for the solitary hermit, and is also, arguably, undesirable in the interests of fostering social interactions and community which can lead to the further growth and development of society.

A common factor identified in privacy debates is the ability of individuals to have control over the release and dissemination of information about themselves. For many this is of crucial relevance to informational privacy. Application of such a control theory suggests that privacy will only be infringed where the individual has not consented to the disclosure i.e. there will be no intrusion on privacy where the individual voluntarily disclosed personal information. Choice is thus an important facet of control as is the power to ensure that the choice is protected. A clear difficulty for the individual is the maintenance of control once information has been voluntarily released since it then passes into the control of others who have no personal interest in protecting that information. Gavison (1980) is critical of the ability to control personal information as being a determinant of the definition of privacy precisely because a dependence on subjective choice makes both a realisation of the scope of the concept and the provision of legal protection problematic. In a quest for a more neutral approach she conceives of privacy as consisting of three components; secrecy, anonymity and solitude. On this analysis, secrecy broadly equates with informational privacy, anonymity is not so much an issue of not being identifiable by name but rather of not being paid attention to and solitude encompasses the physical access aspects of privacy. Privacy is thus objectively deconstructed into constituent parts and total privacy is equivalent to exclusion; nothing is known about the subject, no attention is paid to them and there is no physical access. A logical development is that any interaction will lead to some loss of privacy and an evaluation of the degree of acceptable intrusion becomes necessary. What is deemed acceptable may then depend on the subjective views of the parties. Thus whilst neutral in concept, it is questionable whether this model is any more successful at identifying when legal protection of privacy should occur than a control model.

These represent just a few of the factors which have made privacy and its protection such a hotly contested topic. As Feldman (1994 p. 49) has commented "the problem is that privacy is controversial. The very breadth of the idea, and its tendency to merge with the idea of liberty itself, produces a lack of definition which weakens its force in moral and political discourse." The question in this context is whether the breadth of the idea encompasses the right to anonymity and, if so, what this itself encompasses. A strict meaning of anonymity is not having a name but this is only one aspect of the attention aspect of privacy to which Gavison (1980) refers. We may not know the name of a person but we may know other facts, where people live, work, etc. which can identify them or to make them recognisable to us. These facts taken together with the situations in which we may encounter them means that we can `pay attention' to them sufficient, in particular instances, to amount to an intrusion on their privacy. It is thus possible to conceive of both a wide and a narrow meaning to anonymity. The former, which I shall call complete anonymity, encompasses also identifiability and recognisability whereas the latter relates purely to the attachment of a name.

Use and abuses of anonymity and pseudonymity

The use of anonymous remailers, anonymising software and other related technological developments have made it perfectly possible to wander anonymously (or without label) and also unidentifiably and unrecognisably through Cyberspace. It is even more common to use both traceable and untraceable pseudonyms. To an extent this is also possible in the physical world although the situations when both anonymity and lack of identifiability can be assured are probably not as extensive as might be supposed (see e.g. Lessig (1999 p. 504)). In Cyberspace many personae are possible and the owner of a particular identity may `wander' around as any one of these personae, engage in relationships, be recognised as X, whilst also being known to others as Y or even Z, and where none of these may reveal the individual's `real' identity. Whilst the use of some or many aliases is not restricted to electronic media, it is more problematic in other situations to assume alter egos of different age, sex, ethnicity, status, etc. This is a simple matter in Cyberspace. In more traditional situations there are very few instances where complete anonymity is so easily achieved, some sort of recognisability due to the presence of distinguishing features is the usual situation[1]. In real life the use of formal pseudonyms, though perhaps rarer in general, may be fairly common for a relatively small range of defined purposes - writers, actors and others in the public eye (and this is sometimes more akin to a change of name than to a real pseudonym), and also nefarious activities.

There are many situations in Cyberspace where anonymity or pseudonymity is more usual than in analogous situations in real life. These include participation in fantasy and other games, the use of counselling service and self-help groups, the ability to engage in unrestricted political speech, whistleblowing or other controversial subject without fear of recrimination as well as for more general privacy protection in the course of commercial transactions or to avoid being targeted with requests for assistance etc. Free speech in Cyberspace is more likely to be fostered by anonymity than its counterpart in the real world since features which enable identification can be removed. On the other hand complete anonymity can provide the perfect shield for unlawful or anti-social activity and serious damage is also possible by abuse of pseudonymity. Kabay (1998) cites the example of `Johnny chaotic' who subscribed victims to many newsgroups without their knowledge with the result that they received hundred of unwanted e-mails every day and had to spend time unsubscribing. So both anonymity and pseudonymity certainly make revenge action such as `spamming' and `flaming' a simple matter with little fear of recrimination. Self-appointed net vigilantes may also prefer to hide behind the shield of anonymity whatever their motives.

It is clear that anonymity can be used for good and bad (Froomkin 1996) and, before anonymity is espoused as a panacea for all privacy problems, a balance must be found between the its good effects in enhancing both privacy protection and freedom of speech and the possible disadvantages specifically the protection 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.

Another question is whether anonymity within Cyberspace might, itself, introduce further variables. Over the last century there have been a number of social psychological studies of what has been termed `deindividuation', the state of alienation, reduced inhibition and lack of self-awareness which occurs when a personal sense of identity is overwhelmed and subjected to the group. The work to date has been reviewed most recently by Reicher et al (1998) who trace its origins from the studies of LeBon (1895) on the effect on individuals of submergence in a crowd through to the development of the modern concept of deindividuation. The relationship between anonymity and deindividuation was explored by Zimbardo (1969) who first outlined the observation that anonymity lowered the point at which individuals were likely to indulge in anti-social behaviour. Deindividuated people appear to have less internal control over their behaviour and are also likely to be more influenced by environmental and other stimuli (Diener 1977). They are likely to show reduced inhibition, increased irritability, and an increased incidence of compulsive and reckless behaviour. Although anonymity is a key element, Reicher and Levine (1994) have even suggested that lowered identifiability may be a sufficient trigger for deindividuation.

Bearing this in mind it might be expected that anonymity on computer networks might produce some of the same effects on users. However studies specific to this medium have not always produced consistent results. There has been some apparently convincing evidence of deindividuated behaviour (e.g. Cooper et al (1998)) although it was also noted that despite the increases in the expression of extreme and controversial ideas, one more positive attribute of anonymity in this medium was a reduction in the "stultifying effects of hierarchy". These features had already been alluded to by Sproull and Kiesler (1986) - "... messages are likely to display less social awareness. The advantage is that social posturing and sycophancy decline. The disadvantage is that so do politeness and concern for others." It is also possible that anonymity, rather than causing extreme reactions merely exacerbates existing tendencies. Thus those with conservative tendencies will tend to appear more conservative when communicating anonymously (Rudy, 1996). Siegel et al (1986) noted that computer users "behaved in ways less regulated by self or social norms because cues reminding users of another social presence were absent. This psychological state ... resembled a deindividuated condition similar to that observed in social psychological studies of group behaviour. In a deindividuated condition individuals ... exercise little self-regulation and can act in more aggressive and abrasive ways."

On the other hand, some studies have shown little effects from the use of anonymity (see Valacich et al (1992)) and Greenwood (1992) specifically challenges the assumption that computers create deindividuation within users. But even studies which have produced apparently conflicting results suggest that the effects of anonymity and anonymous communication will also depend on the particular tasks undertaken or other specific circumstances at the time. Thus Valacich et al (1992) concede that they might have found a greater effect if the tasks required in their study had been highly controversial and Cooper et al (1998) point out that "safe topics may not elicit the kind of anxiety for which anonymity may be most telling."

Critics of some of these studies (notably Lea and Spears (1991) and Spears et al (1990)) distinguish personal identity which might be submerged in such conditions from social identity which might be accentuated. They attempt to reconcile the differences between the studies by distinguishing the context in which the activities take place and suggest that some of the studies underestimate the role of social contextual factors.

Despite disputes over explanations and theory, these studies, nevertheless, point to the fact that, specifically in relation to computer networks, individual (and group) behaviour may be modified or even polarised by the effects of anonymity or reduced identifiability. This fact is one which should perhaps not be ignored when evaluating the role of anonymity and balancing the positive and negative effects.

The key issue is perhaps recognisability. In Cyberspace the adoption of numerous personae is a trivial matter and will exacerbate the issue. Further the technology makes true anonymity (incorporating a lack of recognisability, identifiability and traceability) possible in a way which is becoming increasingly difficult to replicate in the real world. A succession of encrypted anonymous remailers makes both identification and traceability impossible for the final recipient.

The legal response

Notwithstanding the activities of cyberstalkers etc., the major concern with privacy on the Internet is with that facet of privacy characterised by Gavison as `secrecy' and frequently referred to as informational privacy. However this has to be balanced with other rights, freedoms and interests most notably freedom of expression and the public interest in law enforcement. There is no clear consensus as to how this can be achieved. In the United States the courts have considered a number of factors in relation to informational privacy. These include the extent to which it could lead to embarrassment and reputational injury which would usually fall to be resolved by the law on defamation; the extent to which it could lead to harassment and/or intrusion such as that referred to above and also the reasonableness of the expectation of privacy.

Perhaps it is not surprising that the courts in the States have not been so concerned with the more basic matters of informational privacy such as the principles governing the collection and processing of personal information which we would refer to by the European term data protection[2]. This is not surprising given the absence of generic data protection legislation and the primary reliance on sectoral self-regulation. In Europe on the other hand, with extensive regulation of data protection, there may be a growing expectation that privacy issues on computer networks are taken care of by the laws on data protection. But it must be remembered that such laws were formulated and drafted to deal with a perceived threat to privacy originating from rather different technology - that of the potential for the abuse of the information contained in large, centralised data banks and there is a very real question over the extent to which these rules can be successfully applied to the decentralised individual activities which characterise the use of the Internet.

Central to the requirements of the 1995 directive (<http://www2.echo.lu/legal/en/dataprot/directiv/directiv.html>) intended to harmonise data protection law in Member States of the European Union is the need for the consent of the data subject except in a restricted number of specific situations. Consent is defined in article 2(h) of the directive as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed". A valid consent, therefore, needs more than an affirmative response, it necessitates the data subject being made aware, at the time the consent is given of the intended purposes of processing, likely use of the data, possible disclosures etc. Although collection and retention of data may be an inevitable consequence of the use of the Internet for many purposes, the correlation of that data with a specific identifiable individual may not be straightforward but, even where it is, the invisibility of the collection leaves little opportunity for informed consent.

Although the Directive is only intended to harmonise the law on data protection within the European Union, it is also having an impact on other jurisdictions because of the requirement in article 25 prohibiting transborder data flow unless the third country has an `adequate' level of protection. Article 25 then gives the Commission responsibility for verifying the adequacy of particular provisions. The US is the first jurisdiction to seek such verification of the adequacy of its proposed `Safe Harbor' principles (<http://www.ita.doc.gov/td/ecom/Principles1199.htm>). This has generated some debate on the meaning of adequate in this context, specifically as to whether it implies that the standard detailed in the directive must be achieved or whether some lower standard will suffice. The draft principles use a voluntary approach based on self-certification and self-assessment and the latest draft has been the subject of a lengthy opinion from the Working Party set up under the Data Protection directive (Working Party 1999b) which was also presented at the European Parliamentary hearing on "The European Union and Data Protection" on 23 February 2000 (<http://www.europarl.eu.int/dg2/hearings/20000222/libe/en/default.htm>). Clearly agreement of this first assessment of adequacy will be of crucial importance in determining the extent to which the 1995 directive is capable of exerting a global effect on privacy policies. Nevertheless a number of commentators appear optimistic about the potential impact of the directive. Bennett (1997 p. 111) has suggested that the "Data Protection directive now constitutes the rules of the road for the increasingly global character of data-processing operations" and Mayer-Schönberger (1997 p.223) predicts that the directive will assist the drive to homogeneity of approach on a global scale.

Whether or not European data protection law is capable of fully protecting privacy rights on global networks is a moot point but it is certainly clear that anonymity would effect such protection during commercial transactions on the open network and as such resolve some of the consumer protection issues raised by the increased and increasing use of e-commerce. Anonymity is therefore being espoused and promoted by a number of intergovernmental and supranational organisations which are active in this area. A recommendation was made by the EC data protection working party (Working Party 1997) that "where the user can choose to remain anonymous off-line that choice should also be available on-line". As we have seen, the situations in real life where complete anonymity occurs are limited and are, arguably, diminishing whereas the availability of complete anonymity on-line is increasing.

The OECD has recommended (<http://www.oecd.org//dsti/sti/it/consumer/prod/cpguidelines_final.pdf>) that the privacy principles enshrined in the 1980 OECD guidelines on data protection should be taken into account subject to the 1998 Ministerial declaration on the protection of privacy on global networks (SG/EC(98) 14/FINAL). This declaration reaffirms the continuing applicability of the 1980 guidelines which are considered to "provide a foundation for privacy protection on global networks". These guidelines do of course articulate principles of good data management but the problems that have already been outlined, of application to invisible data collection, will still apply. The 1998 declaration makes further specific recommendations such as the "encouragement of privacy-enhancing technologies". This is presumably in accordance with the statement in the recitals that users should be "assisted to maintain their anonymity". The declaration notes that further encouragement should be given to the adoption of privacy policies whether implemented by legal, self-regulatory or other means. This is in accordance with the view expressed in the recitals that although there are different approaches to privacy in member countries, these methods can, nevertheless, "work together to achieve effective privacy protection on global networks". Although a common property of many of the provisions in intergovernmental instruments is their striving and aspirational nature this view seems somewhat idealistic, and perhaps even naïve, when viewed in the light of the debate on the `Safe Harbor' Principles. This debate is a consequence of the clash between legal regulation and industry self-regulation. Further the contents of the EPIC report discussed earlier make it clear that, in relation to privacy, there is greater polarisation of views in the US than appears to be the case in Europe. The speculation is that this is due to the familiarity with the effects of legal regulation of data protection which has been present in Europe for some time and has been strengthened by the adoption of the 1995 directive.

The Council of Europe has also made recommendations in this area (Recommendation No. R(99) 5 <http://www.coe.fr/DataProtection/elignes.htm>) which state in the preamble that there is "a need to develop techniques which permit the anonymity of data subjects ... while respecting the rights and freedoms of others and the values of a democratic society." The recommendation later suggests, but does not expand upon, the fact that in some cases "complete anonymity may not be appropriate because of legal constraints" and suggests pseudonymity in such cases.

Conclusions

Despite this activity, the question remains as to whether anonymity is an appropriate standard and to what extent it is essential to privacy protection. Anonymity is certainly not an explicit feature of current data protection law which concentrates more on identifiability. In the on-line world, both the right to privacy and also freedom of expression may be easier to secure by complete anonymity. Disadvantages may be found in investigating criminal activity on global networks and also in potential new problems arising out of the abuse of anonymous use. The decentralised nature of the Internet and World Wide Web makes an assessment and comparison of the risk from the invasion of privacy as against the risk from the difficulty of apprehension of offenders difficult but, in absolute terms, seems essential if a proportionate response to these problems is to be devised. Given some of the difficulties in applying existing data protection to privacy protection on global networks, especially in the absence of consensus on standards between jurisdictions, anonymity can definitely appear an attractive solution.

It is, however, difficult to see that anonymity solves many problems which could not also be solved by use of traceable pseudonymity. This could provide privacy protection whilst not interfering in principle with the policing of illicit activity. It might also reduce the likelihood of deindividuation although this would need further investigation. The problems created by a standard of traceable pseudonymity are practical rather than legal. They include enforcement of the standard given the availability and ease of use of anonymising techniques and choosing a suitable method of tracing. It has been suggested that real identities could be held by service providers but a safe system would need to be carefully devised and controlled although such information would be more obviously subject to existing data protection regimes. In respect of law enforcement clear guidelines would also be required on when the real identity behind the pseudonym could be revealed.

These practical difficulties are by no means trivial and may, in practice, prove insurmountable, so that anonymity, becomes adopted as the most practical solution. It would be reassuring if this was as the result of a considered assessment of all aspects of the problem.

Bibliography

Bennett Colin J `Convergence revisited: Towards a Global Policy on the Protection of Personal data?' Ch. 3 in Philip E Agre and Marc Rotenberg (eds.) *Technology and Privacy: the New Landscape* MIT Press

Cavoukian Ann and Tapscott Don (1997) *Who knows. Safeguarding your privacy in a networked world* McGraw-Hill

Cooper W.H., Gallupe R.B., Pollard S. and Cadsby J. (1998) *Some liberating effects of anonymous electronic brainstorming* Small Group Research vol. 29 pp. 147 - 178

Diener, E. (1977) *Deindividuation: Causes and consequences* Social Behaviour and Personality vol. 5 pp. 143 - 157

EPIC (1999) *Surfers Beware III: Privacy policies without privacy protection*

<http://www.epic.org/reports/surfer-beware3.html>

Feldman, David (1994) *Secrecy, dignity or autonomy? Views of privacy as a civil liberty* Current Legal Problems vol. 47 pp 41.

Fried, Charles (1968) *Privacy* Yale Law Journal vol. 77 pp. 475 - 493

Froomkin A. Michael (1996) *Flood control on the Information Ocean: Living with anoymity, digital cash and distributed databases* <http://www.law.miami.edu/~froomkin/articles/oceanno.htm> also published as University of Pittsburgh Journal of Law and Commerce vol. 15 p. 395

Gavison, Ruth (1980) *Privacy and the Limits of Law* Yale Law Journal vol. 89 pp 421 - 471

Gellman Robert (1997) `Does Privacy law work?' Ch. 7 in Philip E Agre and Marc Rotenberg (eds.) *Technology and Privacy: the New Landscape* MIT Press

Greenleaf, Graham (1998) *An endnote on regulating Cyberspace: architecture vs law?* University of New South Wales Law Journal vol. 21 pp 593 - 622

Greenwood K.E. (1992) *Deindividuation v individuation on the computer* XXV International Congress of Psychology, Brussels July 1992, abstracted in International Journal of Psychology vol. 27 p. 305

Kabay, M.E. (1998) *Anonymity and pseudonymity in Cyberspace: deindividuation, incivility and lawlessness versus freedom and privacy* Annual Conference of the European Institute for Computer Anti-virus Research, Munich 1998
<wysiwyg://4/http://www.icsa.net/library/research/anonymity.shtml>

Lea M. and Spears R. (1991) *Computer-mediated communication, deindividuation and group decision-making* International Journal of Man-machine Studies vol. 34 pp. 283 - 301

LeBon, G (1895) *The Crowd: A study of the popular mind* Ernest Benn (translated 1947)

Lessig, Lawrence (1999) *The Law of the Horse: What Cyberlaw might teach.* Harvard Law Review vol. 113 pp 501 - 549

Mayer-Schönberger Viktor `Generational Developments of Data Protection in Europe' Ch. 8 in Philip E Agre and Marc Rotenberg (eds.) *Technology and Privacy: the New Landscape* MIT Press

Reicher S. and Levine M. (1994) *On the consequences of deindividuation manipulations for the strategic communication of self: Identifiability and the presentation of social identity* European Journal of Social Psychology vol. 24 pp 511 - 524.

Reicher S., Levine, R.M. Gordijn E. (1998) *More on deindividuation, power relations between groups and the expression of social identity* British Journal of Social Psychology vol. 37 pp. 15 - 40

Siegel J., Dubrovsky V., Kiesler S. and McGuire T. (1986) *Group Processes in Computer-mediated Communication* Organizational Behavior and Human Decision Processes vol. 37 pp. 157 - 187

Spears R., Lea M. and Lee S. (1990) *Deindividuation and group polarization in computer-mediated communication* British Journal of Social Psychology vol. 29 pp. 121 - 134

Sproull L. and Kiesler S. (1986) *Reducing social context cues; electronic mail in organizational communication* Management Science vol. 32 pp. 1492 - 1512

Valacich J.S., Dennis A.R. and Nunamaker J.F. (1992) *Group size and anonymity effects on computer-mediated idea generation* Small Group Research vol. 23 pp 49 - 73

Warren and Brandeis (1890) *The Right to Privacy* Harvard Law Review vol. 4 pp 193 - 220

Wacks Raymond (1989) *Personal information: privacy and the law* Clarendon

Wacks Raymond ed. (1993) *Privacy vols. I and II* Dartmouth

Westin Alan F. (1967) *Privacy and Freedom* Bodley Head

Working Party established by article 29 of Directive 95/46/EC (1997) *Recommendation 3/97 Anonymity on the Internet* <http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp6en.htm>

Working Party established by article 29 of Directive 95/46/EC (1998) *On-line services and data protection and the protection of privacy* vol. 1 Annex to Annual Report 1998 European Commission

Working Party established by article 29 of Directive 95/46/EC (1999a) *Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet performed by Software and Hardware* <http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp17en.htm>

Working Party established by article 29 of Directive 95/46/EC (1999b) *Opinion 7/99 on the level of data protection provided by the "Safe Harbor" Principles* <http://www.europarl.eu.int/dg2/hearings/20000222/libe/en/default.htm>

Zimbardo P.G. (1969) *The human choice: individuation, reason and order versus deindividuation, impulse and chaos* in W.J. Arnold and D. Levine (eds.) Nebraska Symposium on Motivation vol. 17 University of Nebraska Press

[1] Greenleaf (1998 p. 594) expresses the opposite view that anonymity is the default for interaction in real life but that some form of identification is usual for Internet communication.

[2] There has been some debate concerning the relationship of data protection and privacy. Interestingly the Data Protection Act 1998 makes no reference to privacy not withstanding its use in the directive which it implements. On the other hand others fail to see any material distinction between data protection and privacy, see e.g. Cavoukian and Tapscott (1997 p. 179) and Gellman (1997 p. 194).