Anonymity and Pseudonymity in Cyberspace: Deindividuation, Incivility and Lawlessness Versus Freedom and Privacy

Paper presented at the Annual Conference of the European Institute for Computer Anti-virus Research (EICAR),

Munich, Germany 16-8 March 1998

by M. E. Kabay, PhD, CISSP
Director of Education
International Computer Security Association

Abstract {back to top}

The growth of the Internet has increased the use of anonymity and pseudonymity in electronic communications. How can Internet users preserve the benefits of privacy while fighting the abuses of a few anonymous and pseudonymous people? In the real world, identity resides in the ways that an individual is recognised and held responsible for her actions; in cyberspace, identity is potentially just a user-ID. Social psychologists have found that anonymity can contribute to deindividuation -- a state of loss of self-awareness, lowered social inhibitions, and increased impulsivity.

The paper suggests practical applications of these insights from social psychology for managers concerned with reducing abusive behaviour by their own employees. In addition, the paper addresses the wider social problem: given the social psychology of anonymity, abuses of the Internet are certain to continue. How, then, shall we collectively respond to continuing incivility and irresponsibility without falling into authoritarian strictures on speech? This paper suggests that a free-market approach using accessibility to communications as a kind of currency may help the Net evolve towards a more civil society. By blocking e-mail from ISPs which fail to enforce acceptable standards for a given community of users, Net users can sort themselves out into groups that tolerate or welcome different levels of anonymity and pseudonymity. No government intervention would be required under such a system.

In addition, this paper suggests a framework for reaching into the early years of the educational system to help integrate cyberspace into the moral universe of children world-wide. The paper argues that in addition to being a moral imperative to support educational efforts on computer ethics, such programs are in the best economic interests of industry, academia and government systems managers.

Anonymity and Pseudonymity in Cyberspace: Deindividuation, Incivility and Lawlessness Versus Freedom and Privacy

1 Introduction {back to top}

As electronic communications technology becomes widespread among increasingly international populations of computer users, one of the most hotly-debated questions is how to maintain the benefits of free discourse while simultaneously restricting antisocial communications and behaviour on the Net. The debate is complicated by the international and intercultural dimensions of communications today; what is viewed as freedom in some parts of the world is perceived as license in other communities. Conversely, what are conceived by some as attempts to impose civility on international discourse are sometimes rejected as gross interference in freedom of speech by others.

At the heart of much of the debate over the advisability and possibility of imposing limits on behaviour in cyberspace is the question of identity. Some of the most egregious abuse of cyberspace seems reasonably to be attributable in part to the ease of concealing identity; using no name or false names, malefactors can often escape almost all of the consequences of their actions.

Corporations and individuals can suffer serious damage to their interests from abuse of anonymous communications. For example, some people have anonymously sent large numbers of e-mail messages to victims in a "mail-bombing" attack. One antisocial person calling himself "Johnny [x]chaotic" subscribed more than a hundred victims to hundreds of mailing lists without their permission in August of 1996; some victims received 20,000 e-mail messages per day from lists dealing with specialised topics in which they had no interest. The victims found it difficult to locate their legitimate e-mail messages in the massive inflow of unwanted information and had to spend considerable time unsubscribing themselves from all the lists (Kabay, 1996).

In 1997, for example (Kabay, 1997), an Annapolis, Maryland woman was mail bombed after she warned other writers about extortionate fees from an author's agency; her name, phone number and address were posted on alt.sex groups on the USENET and resulted in floods of offensive phone calls. A woman in Atlanta was appalled when someone posted a photograph of an unknown anonymous woman with the victim's name and contact information; she received calls from men who told her the announcement claimed she was offering free sex. A victim of such anonymous harassment founded WHOA C Women Halting Online Abuse C to help victims fight this oppression. The CyberAngels, an offshoot of the Guardian Angels vigilante group, claim to be willing and able to help victims.

In Florida, two students posted a picture of one of their high school classmates on a Web site. The boy was pictured dancing with his prom date -- but the girl's head was replaced by the picture of one of their male teachers. An electronic voice on the site announced that the teacher "must die." The student was profoundly disturbed by the intimations of homosexuality, as were the teacher and his colleagues. However, the state attorney's office reluctantly concluded that there is no valid state statute making it illegal for someone to publish libellous information anonymously on the Net. Although Florida does have a law forbidding "anonymous publication of material that holds a person up to ridicule or contempt," the legal experts concluded that such a limitation on speech is unconstitutional.

In January 1997, the self-named "Reverend White," dedicated to making "America straighter and whiter," launched denial-of-service and harassment attack against the widely-used Internet Relay Chat (IRC) channels called the Undernet. "White" and his cronies emitted forged racist and homophobic hate e-mail, overloaded IRC channels and issued threats against users.

An anti-spam activist (a person fighting "spam" -- i.e., unsolicited commercial e-mail), Jim Youll of newmediagroup.com, was mail bombed in mid-May and then his servers were hijacked to send out thousands of junk e-mail messages which in turn led to a huge inflow of abusive complaints from the people being spammed. The frustrated administrator had to spend an inordinate amount of time trying to track down the origin of the attack but got little support from puzzled and largely uncooperative system administrators of intermediate systems involved in the problem. In a similar case, Beth Arnold, an administrator for a small New Jersey ISP (Internet Service Provider), terminated a spammer's account and was then subjected to the consequences of several fraudulent spams in her name. She disconnected her 800 number after receiving 200 abusive calls; she was mail-bombed and her ports were saturated with fraudulent demands for service (SYN-flooded and PING-flooded). She appealed to other ISPs for help in tracking down the anonymous culprit(s) but received no co-operation.

A Web site supporting ETA guerrillas was anonymously mail bombed after ETA killed a Spanish politician. The *Euskal Herria Journal* of New York was pulled off the Web site of the Institute for Global Communications after the IGC's servers were brought to their knees by the flood of duplicate messages and huge binary files sent by opponents of ETA.

An innocent Florida businessman, Bruce Hovland, was harassed by thousands of phone calls from angry strangers who complained about junk e-mail that threatened to bill their credit cards for almost $200 in return for non-existent pornographic videos they had never ordered and did not want. Mr Hovland was the victim of a deliberate smear campaign, probably by a malefactor who had refused to pay rent at Mr Hovland's marina and who had lost his boat in a seizure as a result. The malefactor spammed the net in Hovland's name and suggested that people call his business number collect. Hovland guesses that he lost about two weeks of business because his phones were ringing off the hook. Hovland points out that his case was relatively minor; he imagines the mayhem if an emergency number were posted on the Net in such a fraud. The case illustrates the difficulty for victims in finding an agency willing to receive and follow up on complaints about such outrageous and dangerous attacks.

Unknown hackers assailed the Zip Internet ISP in Sydney, Australia using SYN-flooding and PING flooding. The system was unusable during the worst floods, which are thought to be from local assailants. The ISP was working with federal police in an effort to catch the malefactors. Zip and its backbone provider, connect.com, instituted blocking measures to stem the tide of fraudulent packets.

In November, a surge of fraudulent votes for best college sports song brought down USA Today's Web servers (Elman, 1997). In general, anonymous voting on the Internet has been a dismal failure because of the ease with which Internet users can conceal their identity and automate their votes.

Anonymity is fundamental to the abuse of the Net practised by many spammers. Almost all spam contains forged headers in an attempt to escape retribution; in some cases the forgeries name real domains. One of the most significant cases in the last year began in May 1997, when Craig Nowak, a college student, chose flowers.com at random as the fraudulent return address for his first attempt at junk e-mail. In so doing, he was merely following the suggestions of the unscrupulous purveyors of spam-distribution programs, who usually advise their naive users to forge the headers of their junk e-mail. Unfortunately for his victim, flowers.com is a legitimate business whose owner received 5,000 bounced messages and plenty of abuse for supposedly spamming the world. The enraged florist, Tracy LaQuey Parker, launched a lawsuit for damages and was supported by the Electronic Frontier Foundation (Austin chapter) and the Texas Internet Service Providers Association. In late September, the plaintiffs won a temporary injunction against Nowak and his ISP preventing him from further use of the appropriated domain name (not that he'd have wanted to, at that point). In November 1997, the judge imposed a fine of over $18,000 on the defendants and added a particularly significant passage in her judgement that clearly enunciates the damages caused by forgery of return addresses:

"The Court additionally finds that the Plaintiffs have suffered, and will continue to suffer if not enjoined, irreparable harm in the form of diminution in value of Plaintiffs' domain name; the possibility that Plaintiffs' reputation will be damaged forever by unauthorised use of a domain name associated with them in the controversial and hated practice of Internet spamming; and service disruptions. The potential harm to the Plaintiffs cannot be adequately valued in damages, and therefore the Plaintiffs have no adequate remedy at law. . . . The Court further finds that Plaintiffs . . . suffered actual damages from the unauthorised actions of the Plaintiffs, including lost time, lost income, lost business opportunities and lost use of their respective computer systems."

In light of the seriousness of these abuses of inadequate identification in cyberspace, system managers and others concerned with the continued success of the Internet as an effective communications medium should consider the reasons for abusive behaviour of anonymous individuals. Is such abuse an aberration particular to cyberspace or are there precedents in history and in other areas of life that can provide insights to shape public and corporate policy towards identification in cyberspace?

This paper reviews some of the findings of social psychology that show how anonymity has generally been associated with antisocial behaviour. It is the contention of the author that anonymity on the Net will inevitably continue to spawn antisocial behaviour in cyberspace and that we must somehow manage to integrate this kind of abuse into our plans for the further development of the Internet. The paper then presents some practical ways system managers can encourage employees in their own organisations to use the Net responsibly. Some practical suggestions on how different degrees of tolerance for anonymity can be integrated into a cyberspace polity are discussed.

2 Definitions {back to top}

Before plunging into an exploration of anonymity in cyberspace, it will be helpful to establish some common vocabulary. What is cyberspace? What is identity and its absence? What is pseudonymity?

2.1 Cyberspace

In this paper, "cyberspace" means the totality of electronic data storage and transmission; this paper will focus on communications using the Internet. On the Internet, there are users of specific domains defined in the Domain Naming System (DNS) such as companies (e.g., those using addresses ending in ".com"), universities and other educational institutions (e.g., ".edu" addresses), US government agencies and departments (".gov"), the US military (".mil"), and network service providers (".net"). There are many geographical domain names such as those ending in ".de" or ".uk" which include users from commercial, educational, government and military organisations. In addition, there are many Internet Service Providers (ISPs) in the .net and .com domains in the United States and throughout the world in geographical domains whose members communicate through the Internet. Customers of Value Added Networks (VANs) such as America Online (AOL) and CompuServe (CSi) communicate through the Internet as well as having restricted areas within their VANs where only members can post messages and files. All Internet users can post messages in public discussion lists on the Usenet or through remailing lists which broadcast all inbound e-mail to participants. Henceforth, for convenience, "the Internet" or "the Net" will include any of these users. Users of direct-dial bulletin board systems and modem-to-modem direct links are explicitly excluded from this discussion.

2.2 The real world

Also for convenience, "the real world" refers to the material, physical, atomic and molecular world of everyday human interactions. Using "real-world" in this way is not intended to imply that cyberspace is less significant, useful or even "real" than the planetary level on which we interact; it is merely a convenient reference to distinguish the physical from the electronic.

2.3 Identity in the real world

The key meanings of the noun "identity" for our purposes are defined in a dictionary (American Heritage, 1992) as (quoting directly):

1) The collective aspect of the set of characteristics by which a thing is definitively recognisable or known;

2) The set of behavioural or personal characteristics by which an individual is recognisable as a member of a group;

3) The distinct personality of an individual regarded as a persisting entity; individuality.

2.4 Anonymity and pseudonymity in the real world

Clarke (1997b) summarises the importance of personal identification as follows:

"The purposes of the interchange of identification include

to provide a gesture of goodwill,

to develop mutual confidence, and

to reduce the scope for dishonesty;

to enable either person to initiate the next round of communications; and

to enable either person to associate transactions and information with the other person."

Anonymity can be defined simply as being without a name or with an unknown name. *Pseudonymity* is the use of a false name. These terms are imbued in English with a negative connotation; nonetheless, anonymity has an honourable history in world philosophy and politics. In the United States, for example, the seminal *Federalist Papers*, which appeared in 1787 under the pen-name "Publius," is a publication held up as a shining example of

anonymous contribution to political thought (Froomkin, 1995).

Clarke (1997b) explores the concepts and history of human identity in a section of his paper on management and policy issues relating to human identification. Individuality has been a central concept in Western civilisation since the Renaissance, says Clarke. However, individuals can adopt more than one identity; for example, some women use their husband's surname in private life but maintain their original family name in their professions (Clarke, 1997b). Some people have several identities; e.g., novelists with different styles sometimes use various pen-names. The Danish philosopher Srren Kierkegaard wrote under sixteen pseudonyms; Charles Dodgson wrote as Lewis Carroll; Eric Blair wrote as George Orwell. As the work of these writers illustrates, anonymity and pseudonymity are not inherently linked to antisocial behaviour.

3 Social psychology of anonymity {back to top}

Technological change can have profound consequences on social behaviour. For example, the development of mass-produced automobiles made possible the development of suburban shopping malls in the United States which in turn have led to an adolescent mall-culture unimaginable in the 1920s (Froomkin, 1995). Most of us have ourselves observed that driving an automobile can alter a person's behaviour from civility to incivility; in some cases, otherwise normal people become violent when they are behind the wheel of a car (Free, 1997).

It seems quite likely that the pervasive spread of the Internet will have equally profound effects on social organisation and interactions. We should study what is already known about the effects of anonymity as we analyse anonymity in cyberspace. The following sections review some well-established information on anonymity and social behaviour from the social psychology literature. The implications of these principles for individuals, corporate policy makers, ISPs and governments are discussed in the final section of the paper.

3.1 Deindividuation theory

What do scientists know about the behaviour of anonymous people? In general, the findings are not encouraging for the future of cyberspace unless we can somehow avoid the known association of antisocial behaviour and anonymity.

Early work on people in groups focused on anonymity as a root of the perceived frequency of antisocial behaviour (Le Bon, 1896). The anonymous members of a crowd show reduced inhibition of anti-social and reckless, impulsive behaviour. They are subject to increased irritability and suggestibility. One wonders if the well-known incidence of *flaming* (rude and largely *ad hominem* communications through e-mail and postings on the Usenet and other public areas may be traceable to the same factors that influence crowd behaviour.

Later social psychologists formulated a theory of deindividuation (Festinger et al., 1952) in which they proposed that one's personal sense of identity can be overwhelmed by the sense of belonging to a group. Zimbardo (1970) suggested that anonymity, diffusion of responsibility and arousal contributed to deindividuation and antisociality. He noted that deindividuated people display reduced inhibitions, reduced reliance on internal standards that normally qualify their behaviour, and little self-awareness.

3.1.1 Deindividuation and technology

As mentioned briefly in the introductory comments for section 3, there is some reason to suppose that technology can contribute to the deindividuation of its users.

Anonymity has been postulated in anecdotal reports to account in part for the strong contrast in behaviour of normal people who become aggressive and hostile when driving cars (Free, 1997; Russell, 1997). It seems intuitively plausible that being isolated in a tight personal space, a cocoon of glass and metal, gives some drivers a feeling of power precisely because of their (possibly temporary) anonymity. In addition, the anonymity of the other drivers may lead to a kind of dehumanisation of the other. It would be interesting to study how many angry drivers refer to "that car" instead of "that driver" when they rail against some random act of road rudeness. Similarly, it seems to this writer that the isolation of an Internet user may also contribute to aggressivity; the object of wrath may, much like the driver of another car, be dehumanised. Sometimes it seems that e-mail flamers are engaged in their version of a video game; they give the impression of losing sight of the real human beings on the other end of their verbal

aggression.

Writers of computer viruses and others in the criminal computer underground may also focus so intensely on the challenge of defeating machines that they lose sight of their human victims. Criminal hackers have expressed themselves as attacking systems, not people; in personal interviews with young hackers at a hacker conference, this writer was struck by comments such as, "Oh, I would never steal anything from a person, but if I found a radio in an office and it were labelled with a company sticker I wouldn't think twice about taking it." A commonplace informal interpretation of the insouciance of hackers and virus writers is that they are subject to what is laughingly called the "video-game syndrome:" they seem to focus on their actions as if they were part of a game with only computers on the receiving end.

3.1.2 Anonymity and aggression

Sometimes anonymous people go beyond verbal abuse and seem to be willing to inflict harm on others.

Experimental work by Zimbardo (1970) suggested that anonymity can significantly increase aggression. For example, when women were asked to deliver electric shocks to victims, those who agreed to wear white lab coats and hoods administered what they thought were longer shocks to the supposed victims compared with women who wore their own clothes and name tags.

In a cross-cultural study, Watson (1973) analysed the correlations between the ritual, anonymising costumes and war-paint of warriors and their style of battle and post-battle treatment of prisoners. He found a strong positive relationship between anonymity and brutality.

Violent soccer fans seem to be disinhibited in part because of the anonymity of the crowd (Kerr, 1994). In a personal undercover investigation, a journalist found that anonymity and pseudonymity are integral components of the antisocial behaviour of soccer hooligans (Buford, 1991).

These findings suggest that so-called "dark-side hackers" may significantly be influenced in their willingness to cause damage to computer systems and networks precisely because their very anonymity influences them to cross normal behavioural boundaries. These people may not be permanently, irremediably damaged human beings they sometimes seem; they may be relatively normal people responding in predictable ways to the absence of stable identification and identity.

3.1.3 Anonymity and dishonesty

Does anonymity increase the likelihood that people will transgress rules and laws? Apparently yes.

In an experiment involving children, young trick-or-treaters were asked to take only one candy from a bowl and then left alone or in groups, supposedly unobserved. Those children who had given their names to adults were observed to be far less likely to take extra candy or to steal coins than those who had remained anonymous (Diener et al., 1976) even when the adults were apparently away.

As we can see, the effects of anonymity on youngsters may be a serious problem for system administrators who are under siege by under-age hackers.

3.1.4 Deindividuation and self-awareness

Why does anonymity change people's normal inhibitions and influence them to behave abnormally? It seems that the deindividuation of anonymous people lowers their self-reflective propensities.

Exploration of the inner world of deindividuated people suggests that they are less aware of themselves and may even enter a state of altered consciousness (Prentice-Dunn & Rogers, 1980; Diener, 1979). Prentice-Dunn and Rogers studied the behaviour of college men who, as in the work of Zimbardo (1970) cited earlier, were asked to administer what they thought were electric shocks to confederates of the experimenters who were masquerading as victims. Some subjects were subjected to dim lighting and loud background noise; their names were not used; and they were told that the levels of the shocks they gave would not be recorded. These subjects were thought to be deindividuated. Other subjects experienced bright lights in quiet rooms; they were called by name; and they were

told that their shock levels would be monitored. The deindividuated subjects administered more severe shocks to their victims than the individuated students.

These observations may tie into the work on *autotelic* experiences (Csikszentmihalyi, 1990) and the loss of self-awareness that can occur in repetitive, challenging, feedback-rich activities such as programming (or perhaps virus-writing) and criminal computer hacking. Csikszentmihalyi studied people in a variety of work environments and in their home life and hobbies. The subjects reported on their attainment of a state of timelessness, where the passage of time was insensible. Many of us who have programmed know how easy it is to forget to eat or to go home when we are deeply involved in our work; similarly writers and musicians can lose track of time. The research suggested that some of the key attributes of an activity that leads to this autotelic experience are rapidity of feedback (e.g., seeing an article growing as one writes or running an increasingly complex program under development) and being at the limits of one's abilities. Challenges that are too easy and too hard both prevent the loss of self-awareness that defines the autotelic state.

Several recent popular books dealing with criminal hackers have mentioned the ability of legendary hackers to stick to their hacking for hours on end as if they were entranced. Combine the autotelic nature of hacking with the deindividuation associated with anonymity and we have a prescription for trouble.

3.1.5 Anonymity and pro-social behaviour

The picture is not necessarily all bad, however. Sometimes a different context can liberate anonymous subjects from their counter-productive inhibitions.

In some cases, it can be shown that anonymity has an unusual effect: to increase prosocial behaviour instead of increasing antisocial behaviour (Spivey & Prentice-Dunn, 1990). Gergen et al. (1973) put people into brightly lit chambers or in totally dark chambers and monitored the behaviour of the strangers they had put together; in the dark room, there was much more uninhibited and positive expression of physical contact such as hugs and of emotional openness such as discussions of personal matters. However, directionality of these effects may be affected by the demand-characteristics of the situation. That is, the way the experimental objectives were described could cause significant differences in the subjects' behaviour.

The constructive, supportive communications often seen in discussion groups dealing with substance abuse, abusive relationships and other personal and interpersonal problems illustrate the possible benefits of anonymity in a positive context.

3.2 Identity in cyberspace

What exactly do we mean by identity when we are using electronic communications? Is one's e-mail address an identity? Could a made-up name be an identity?

Identity on the Internet is primarily the e-mail address (Detweiler, 1993). The e-mail address sometimes provides crude and unreliable information about affiliation (e.g., domain names .gov, .mil, .edu) and geographic location (e.g., .ca, .uk, .fr) (Detweiler, 1993). Roger Clarke, a scholar with a long professional interest in questions of identity, identification and privacy in cyberspace, has written an excellent introduction to these questions (Clarke, 1997a). For discussions of information technology, Clarke defines "identification" as "the association of data with a particular human being." (Clarke, 1997b)

3.2.1 The theory of nymity

There has been considerable discussion on the Net about the kinds of identity that people assume in cyberspace. One of the best-known writers on this subject was "L. Detweiler;" it is still unknown whether this was a real name (Anonymous, 1996a and 1996b). Detweiler suggested that identity on the Internet is amorphous and unstable because there is no one-to-one relationship between people and e-mail addresses. One person may use multiple e-mail addresses and many people may share a single address (Detweiler, 1993).

Detweiler conducted a vigorous battle against what he perceived as a sinister and deceptive practice he called pseudospoofing. Pseudospoofing, in Detweiler's conception, is the use of multiple aliases by an individual or a

conspiracy; these aliases allow the perpetrators to deceive observers into misjudging the number of people agreeing or disagreeing over specific positions (Anonymous, 1996). One of the literary sources for such a practice is the science-fiction book, *Enders Game*, by Orson Scott Card (Anonymous, 1996a; Card, 1985). That author posits a galactic political debate in which two individuals distort political debate by engaging in erudite polemics using pseudonyms; but they also invent subsidiary personae that agree or disagree with the main pseudonyms. These subsidiary personae lend credibility to the desired winning side by offering support or by deliberately poor arguments and attitudes. Their number convinces politicians to pay attention to the debates.

A current illustration of the problems of pseudospoofing is the widespread difficulties experienced in online voting. The ease with which identity can be created, coupled with the ease of automatically scripting multiple votes, leads to thoroughly unreliable tallies in almost all online polls. The only way to avoid such abuses is to enforce some tight coupling of real-world identity with the electronic identity registered for voting. Perhaps biometric identification will eventually be the only acceptable form of authentication for voting online.

3.2.2 Types of anonymity and pseudonymity

To understand the problem of anonymity and pseudonymity, it is useful to define varying degrees of the behaviour. Froomkin (1995) distinguishes among four forms of imprecise or absent identification:

1) Traceable anonymity: any anonymous remailer that keeps a record of the relation between the original message and the anonymised message allows tracing.

2) Untraceable anonymity: no record is kept or available showing the origin of an anonymised message.

3) Untraceable pseudonymity: a continuous identity or persona allows communication with a correspondent but there is no way to link the pseudonym to the correspondent's real-world identity.

4) Traceable pseudonymity: someone, somewhere has the information required to complete the link between a pseudonym and a real-world identity.

The "anonymising" remailer anon.penet.fi was actually a *traceable pseudonym* remailer. When a message was received by the server, its headers were stripped and it was assigned a fixed random pseudonym. In order to allow replies to the pseudonym to be forwarded to the original sender, every pseudonymous identity was linked in a table to the original e-mail address. When Finnish police ordered Johan Helsingius in 1995 to identify the pseudonymous poster of copyrighted Scientology texts on the USENET, Helsingius felt obliged to reveal the link (Froomkin, 1995).

Traceable on-line anonymity allows people to maintain their privacy by using screen identities, but many ISPs will furnish the real-world identity to law-enforcement officials with a warrant or to tort lawyers with a subpoena. AOL, for example, furnished subscriber details to the lawyers for a Caribbean resort considering a lawsuit for defamation based on postings by "Jenny TRR" on AOL (Johnson, 1995). All the ISPs that charge money for access are inherently providing traceable pseudonymity even when they permit false screen names.

Larry Lessig, David Post and Eugene Volokh also distinguish between anonymity, pseudonymity and traceability in their Internet course on cyberspace law (Lessig et al. 1997a). They emphasise that private organisations such as Internet Service Providers can freely set terms of service that allow or forbid anonymity, but they may be required in the United States to provide traceability if the courts require it for individuals (Lessig et al. 1997b).

In general, it is difficult to see how the rule of law can apply to cyberspace without some form of traceability. Whether civil law or the criminal law is involved, the defendant must be found for court proceedings to have any effect. Untraceable anonymity and untraceable pseudonymity preclude justice for the aggrieved parties. Clarke (Clarke, 1997a) points out that privacy interests are always to be balanced with other interests such as the public good, commercial interests, and the interests of other individuals. For example, the desire to post anonymous libel (construed as privacy of personal behaviour) conflicts with the desire of the victim to be free from libel; anonymity makes it impossible to use the civil law for redress.

3.2.3 Why anonymity and pseudonymity are commonplace in cyberspace

Surely anonymity and pseudonymity are possible using older means of communication: people have thrown rocks

through windows, sent anonymous vituperation through the mail, and harassed people with anonymous phone calls for millennia, centuries and decades respectively. Such behaviour has historically been of relatively minor importance. How is it that anonymity and pseudonymity seem so important in cyberspace?

One factor is the ease with which one *can* be untraceably anonymous in cyberspace. Many ISPs allow users to define screen-names or aliases; some ISPs such as AOL have distributed millions of trial subscription disks that allow one to create an identity and then dispose of it after fifty hours online. Anonymous remailers permit users to send e-mail to a central address where all identifying information is stripped and the original text is then retransmitted to the desired destination. Some moderated USENET groups and e-mail-based mailing lists require a "real" name but there is little effort or even possibility, as things currently stand, for authentication of such names. Unmoderated groups, by definition, do not require real names at all; these allow postings by anyone. Almost all the contributions to counter-cultural or frankly criminal Usenet groups and distribution lists are anonymous or at best pseudonymous.

In addition, some people systematically forge the headers of their e-mail, often introducing completely false addresses for their origin but occasionally picking real addresses, whether by accident or design (Pappas, 1997). Forging e-mail headers can conceal the true origin of a message (Detweiler, 1993). Junk e-mail almost always includes false return addresses.

Another way to generate false header information is to compromise someone's e-mail account. If security on an e-mail address is compromised, messages can be forged with a false ID (Detweiler, 1993).

The other factor that makes anonymity and pseudonymity especially significant in cyberspace is the ease of replication of messages. An anonymous communicator could hope to reach at best a few dozen or hundred people in a day with the phone system or by mail; in most areas, each phone call or letter would cost something to send. In contrast, outbound electronic mail and postings to Usenet groups generally cost the originator nothing.

4 Balancing rights and duties {back to top}

Is there a basis for evaluating the ethics of using anonymous and pseudonymous communications? Are these modes of communications protected by principles of privacy, for example?

4.1 Benefits of anonymity and pseudonymity

In discussions of whether society ought to restrict anonymity and pseudonymity, a common argument is that these modes of communication are necessary to fight tyrannical corporate and political institutions. Anonymity and pseudonymity are, in this view, expressions of the right to privacy. Abuses are the price society has to pay to preserve the benefits of these tools of expression. The following sections examine the concepts of privacy and the resulting benefits of anonymity and pseudonymity.

4.1.1 Privacy in cyberspace

If privacy rights are claimed to protect anonymous and pseudonymous communications, it is important to understand the concepts of privacy.

Clarke (Clarke, 1997a) defines privacy as, "the interest that individuals have in sustaining a 'personal space', free from interference by other people and organisations." He analyses the concept further, naming four dimensions of privacy:

1) Privacy of the person: freedom from compulsory tampering with one's body.

2) Privacy of personal behaviour: freedom in such matters as sexual preferences, religion, and politics.

3) Privacy of personal communications: freedom from routine monitoring of interpersonal communications.

4) Privacy of personal data: control over who can obtain and what can be done with personal information.

Political discussion groups, resistance to totalitarian regimes, and discussions of socially-embarrassing or traumatic

problems are made easier for many people by the use of pseudonyms or of anonymity. Anonymity permits unrestricted political speech, whistle-blowing with reduced likelihood of retaliation, and public or private discussions of potentially embarrassing personal problems (Froomkin, 1995, 1996). Ubois (1995) writes, "Anonymous communications are helpful in many ways. They've long been a tool of suicide prevention hotline, suggestion boxes, and personal ads. Anonymity assures privacy, confidentiality and security for individuals. But it also highlights the clash of interests between the individual and the community. Under a repressive government, it's a vital tool for keeping discourse alive. Just consider that Tom Paine would have landed in prison shortly after the publication of Common Sense if his identity hadn't been kept a secret."

In chat rooms and multi-user dungeons, anonymity permits a flowering of imaginative departures from the strictures of participants' real-world identity, social status, personality, gender and gender preferences, political affiliation, national origins, and religion. Multimedia environments such as WorldsAway (http://www.worldsaway.com/home.shtml) provide an imaginative pseudonymity by allowing each player to select a stable name and a pictorial representation of themselves (an *avatar*) with amusing and fanciful features (various imaginary animal heads, skin colours, body shapes and so on). Players adopt personae that can be quite different from their real-world identities, yet there is a consistent identity within the virtual world. Because of this consistency, social mechanisms have arisen in these worlds; e.g., avatars can be invited to join parties if they are perceived as friendly or excluded and shunned if they have violated the norms of the imaginary world.

Anonymous, invisible electronic personalities can escape some of the damaging effects of intolerance and prejudice (Detweiler, 1993). Everyone probably knows of a famous cartoon showing two dogs at a terminal, one of whom is saying, "On the Internet no one knows you're a dog." For example, some professors may spend more time and effort in discussions with undergraduate students if they don't realise whom they are corresponding (Detweiler, 1993). At an intellectual level, stripping the authors of published materials of all details of their age, sex, race, national origin and other attributes can reduce the effects of prejudice and focus discussion on substance. Absent such details, correspondents must perforce focus on the texts rather than on personalities (Froomkin, 1996).

In electronic commerce, anonymity is a prerequisite for successful implementation of some trading systems (Froomkin, 1996). All electronic or digital cash schemes (*e-cash*) emphasise the value of anonymous transactions for safeguarding consumer privacy.

In a legal sense, anonymity and pseudonymity are analogous to limited liability -- a concept familiar from the business world. In business, people pool their assets into a limited-liability partnership or other form of collectivity to prevent seizure of all their private assets if their collective entity becomes liable for debts or penalties (Post, 1995). Perhaps cyberspace anonymity and pseudonymity can encourage collective publications in an analogous way; e.g., Post and others have formed The Cyberspace Law Institute. Some members would be reluctant to participate if their real-world identities were known to the public.

We therefore see that anonymity and pseudonymity cannot reasonably be forbidden without the loss of important benefits to individuals, corporations and society at large.

4.1.2 Defeating dataveillance

Another area where anonymity and pseudonymity have marked benefits is in preventing intrusive monitoring of individual behaviour in cyberspace. Clarke (1997a) has defined *dataveillance* as surveillance using electronically compiled information about a person. The growth of some kinds of electronic commerce will increase pressures for strong identification and authentication (Detweiler, 1993); anonymity serves to protect privacy in a world of electronic commerce. For example, without anonymous digital cash, it would be easy to accumulate detailed records of every electronic purchase made by an individual. Complete knowledge of purchasers' interests can be unfair for customers; for example, knowing that a user is addicted to fantasy simulation games, a retailer may neglect to offer that person a discount -- or may even increase the price of the next game (Froomkin, 1995).

Froomkin (1996) summarises the issues well in his magisterial review of the challenges of anonymity in cyberspace:

"Anonymity lies at the heart of three interrelated problems arising from computer-aided communications over distributed networks (which I will call "the Internet" for short). First, communicative anonymity is an issue in itself: the Internet makes anonymous communication easy, and this has both good and bad consequences. . . .

Second, the availability of anonymous electronic communication directly affects the ability of governments to regulate electronic transactions over the Internet (both licit and illicit).

Third, anonymity may be the primary tool available to citizens to combat the compilation and analysis of personal profile data, although data protection laws also may have some effect also. The existence of profiling databases, whether in corporate or public hands, may severely constrict the economic and possibly even the political freedoms of the persons profiled; although profiling may not necessarily change the amount of actual data in existence about a person, organising the data into easily searchable form reduces her effective privacy by permitting "data mining" and correlations that were previously impossible."

Froomkin discusses digital cash as an application of electronic anonymity and emphasises the potential for abuse by "The Argus State" if anonymity is not guaranteed for readers. For example, he points out, in the absence of anonymous digital cash, reading texts on the Internet using micropayments for each access could provide a traceable record of a person's interests. Such records would be a gold mine for repressive regimes world-wide.

Again, we have to admit that trying to ban anonymity and pseudonymity would have serious disadvantages for everyone, not just the benefits of impeding abuse by a minority of antisocial users.

4.2 Disadvantages of anonymity and pseudonymity

At this point, having looked at some of the benefits of anonymous and pseudonymous communications, let us turn to how several commentators have viewed the abuses of these modes of communication.

Returning to our example of the benefits of having a professor communicate with a student because of anonymity, one can point out that misrepresentation of identity by such an undergraduate manipulates a professor into a decision based on a falsehood (Detweiler, 1993).

Widespread use of untraceable e-cash may lead to increased fraud, tax-evasion, money-laundering, extortion, blackmail and kidnapping (Froomkin, 1995). Some crimes where solicitation leads to potential blackmail -- e.g., hiring a murderer -- may become easier with anonymity and untraceable e-cash. Industrial sabotage by anonymous publication of trade secrets can damage organisations; e.g., the publication of RC4 algorithms from RSADSI has lowered the monetary value of the algorithm. Froomkin writes, "[The] inability to redress legitimate claims is, I believe, the strongest moral objection to the increase in anonymous interaction."

Jurisprudence in the United States has generally supported claims to a right of anonymity in political speech. However, there have been several precedents where anonymity used to cloak socially harmful acts has been stripped from the perpetrators. Perfect (untraceable) anonymity prevents society from bringing sanctions to bear on malefactors (Post, 1995).

Detweiler (1993, 1997) suggested "that Internet anonymity is a bad thing [and] that all user accounts should lead back to real users in the hopes of improving online behavior, especially in chat systems and the like." He responded to critics who claimed that "anonymity is an important part of life and ought to be part of the Internet as well" by pointing out that in real life, anonymous people cannot engage in such activities as opening a bank account, getting a driver's license, getting telephone service, or buying insurance coverage. He concluded, "So grow up and accept responsibility for what you do on the Internet."

Rose (1994), well-known in cyberspace law circles, writes scathingly of the seamier applications of on-line anonymity:

"People can anonymously transmit all sorts of illegal and injurious materials into public areas: copyright infringements, obscenity, stolen credit information, lies and slander, and so on. Individuals with a bone to pick against anyone else can get their licks in without fear of reprisal. Anonymous remailers are great for cowards. People who want to spread messages of hate and misunderstanding, but are unwilling to stand behind their views in public, can operate behind a wall of complete anonymity and inject a strong dose of thought pollution into the public arena."

Another argument supporting disclosure of the origins of speech is quoted by Froomkin (1996), ironically from an

anonymous author: "'Disclosure advances the search for truth,' because when propaganda is anonymous it 'makes it more difficult to identify the self interest or bias underlying an argument.'" Libel on the Internet is particularly pernicious, since once anything has been circulated via the Net, it becomes impossible in practice to destroy all the copies that may reside on numberless computers around the world.

The imaginary Good Times "Virus" supposedly destroys hard disks as soon as the victim reads an e-mail message; Craig Shergold was once a sick child in England who asked for postcards -- and is now heartily sick of the bagsfull of cards he receives daily; and "Jessica Mydek" claims to be an appeal on behalf of an unfortunate girl (but she never existed).

The resurgence of hoaxes and rumours such as the Good Times "Virus" and the pathetic stories of Craig Shergold and Jessica Mydek illustrate the persistence of undated, unsigned and untrue messages in Cyberspace. These unfounded, exaggerated or obsolete stories, threats and appeals circulate endlessly among the gullible on the Net. There is no reason to suppose they will ever stop.

One of the significant lessons from e-mail hoaxes and chain letters is that unsigned, undated correspondence is always to be treated with scepticism. This principle of devaluing anonymous or pseudonymous communications will be used later in this paper in a model for categorising and sequestering communications as a function of their traceability.

5 Systems analysis of nymity {back to top}

Why can't the usual protections of the criminal and civil law deal with anonymous and pseudonymous communications? This problem is addressed by David Post and David Johnson.

Post and Johnson argue that geographically-defined nation-states cannot reasonably cope with a virtual, boundary-less communications medium (Post & Johnson, 1997). In the real world, geographical clustering combines with basic concepts of consent of the governed through some form of representation to legitimise the exercise of state power. Without the consent of the governed, state power fades insensibly into state tyranny. In their requirements analysis of possible systems of governance of cyberspace, they add that wherever possible, those affected by the conduct to be regulated have some say in framing the regulations.

However, in cyberspace, argue Post and Johnson, there is no geographical clustering. There is no "here" or "there" in cyberspace. "Location is indeterminate because there is no necessary relationship between electronic addressing . . . and the location of the addressee (machine or user) in physical space."

Post and Johnson applied the work of the scientist Stuart Kauffman on self-organising systems to study the nature of rule-making in a complex system that can model the interactions among users in cyberspace (Post & Johnson, 1997; Kauffman, 1993). Research on self-organisation of complex systems suggests that optimum configurations of constraints (regulations) can evolve when there is some degree of aggregation (they refer to "patches") in the population. These aggregates represent groups where individuals sacrifice some of their preferences in return for overall improvement in the way the whole society works. Members of a patch share responsibility for governing their behaviour.

One of the most striking findings of Post and Johnson's research is that systems where most of the effects of an individual's actions are felt by others outside its decision-making unit lead to chaos or to suboptimal configurations of rules. Contrariwise, a balance between bringing consequences to bear on individuals in a "patch" and allowing effects to propagate through the larger population leads to more optimal results in the system.

As a result of the experiments, Post and Johnson suggest that one of the most powerful tools for rebuilding comity in cyberspace is grouping users by their Internet Service Providers. Each ISP can develop its own rules governing the behaviour of members; sanctions for transgression of these local rules would include banishment from the ISP.

The authors examine the case of unsolicited commercial e-mail ("spam"). As long as each ISP enforces technical measures against allowing fraudulent origination addresses, everyone in cyberspace can decide whether or not to filter out messages from any given ISP. ISPs that allow behaviour judged harmful by others will limit the range of communication of their members.

Those that are viewed as restrictive will self-select their own members accordingly. Thus without any global legislation, simply allowing individuals to choose ISPs that have published rules they like could lead to an effective self-regulation of communications. In essence, loud-mouthed rumour mongers would end up talking only to each other; junk e-mail could be identified simply from its provenance; and even copyright violations could be punished by collective banning of communications from the offending ISPs.

Such a model is an instance of the ideal "market of ideas" in that objectionable ideas are not forbidden, they are just ignored. Of course, admirable and desirable ideas may also be ignored, but at least there is a choice involved. Access for communication becomes a form of currency in such a model -- perhaps appropriate for the governance of cyberspace, the realm of electronic communications.

6 Implications and Discussion {back to top}

Any attempt to restrict anonymity on the Internet would inevitably affect pseudonymity as well (Post, 1995). Anonymity and pseudonymity make law enforcement difficult enough, but these difficulties are exacerbated by the jurisdictional problems caused by a thoroughly decentralised communications medium like the Internet; "[W]ho should be setting the rules that apply to this new global medium?" (Post & Johnson, 1997).

What, then, are some of the practical measures we can individually and collectively take to preserve the benefits of anonymity and pseudonymity without suffering the consequences of abuse? In the following sections, I try to draw together the implications of the ideas presented above.

6.1 Individuals, families, and schools

Defining normative behaviour begins in earliest childhood and continues throughout the development of the child's capacity for rationality and ethical judgement. I think that children should be taught that anonymity and pseudonymity are not acceptable under normal circumstances. The same methods that parents, teachers and other adults use to teach children a visceral dislike of antisocial behaviours such as lying, cheating, stealing and bullying should be applied to behaviour in cyberspace. As I have written in another work (Kabay, 1994),

"It takes time to integrate morality into our technological universe. Twenty years ago, many drivers felt that driving under the influence of alcohol was adventurous. Today most people feel that it's stupid and irresponsible. Smoking in public is becoming rare. Many of us in northern cities have witnessed exiled smokers huddled together in the cold outside buildings where they once lit up with impunity.

Similarly, we need a consensus on good behaviour in cyberspace.

Criminal hackers who break into computer systems and roam through users' private files should be viewed as Peeping Toms. Criminals using computers to extort money or steal services should be recognised as thieves. Those who destroy records, leave logic bombs, and write viruses should be viewed as vandals. Hackers who smear obscenities in source code should be seen as twisted personalities in need of punishment and therapy. Government agencies proposing to interfere in electronic communications should be subject to scrutiny and intense lobbying.

Beyond such prohibitions and inhibitions of taboos, cyberspace needs the electronic equivalent of Emily Post. We need to discuss the immorality of virus writing, the ethical implications of logic bombs, and the criminality of electronic trespassing. We should teach children how to be good citizens of cyberspace and not just in schools. We should sit down with computer-using youngsters and follow them through their adventures in cyberspace. Parents should ask their teenage whiz-kids about hacking, viruses, software theft and telephone fraud. We must bring the perspective and guidance of adult generations to bear on a world that is evolving faster than most of us can imagine.

The adolescent confraternity of criminal hackers and virus writers have already begun developing totems: the personae of Dark Avenger and Acid Phreak loom over youngsters much as Robin Hood once did for another generation.

What we need now are taboos to match the totems."

6.2 A framework for ethical analysis

For older children and adolescents, the decision to adopt anonymity or pseudonymity is amenable to ethical analysis just like any other decision affecting other people. Kallman & Grillo (1996) have provided a framework for ethical decision making that is focused on decisions in the use of information technology. In a few pages, they provide a clear, accessible set of questions to help anyone make ethical decisions; their book is so clearly and simply written that it would be useful for anyone who uses the Internet. In addition to providing a basis for discussions within corporations and government, the book could also provide the basis for hours of interesting discussion in families who care about what their older children are doing to themselves and to others in cyberspace. The textbook would serve admirably for high-schools as it does for college classes. Perhaps adaptations of this text could be written to help elementary-school teachers approach such issues with younger children.

Kallman & Grillo's framework is easily applied to anonymity and pseudonymity. The following is a transcription of Figure 3-1 in Kallman & Grillo's book:

Approaches to Ethical Decision Making

Law and Ethics

Does the law provide an answer? (Professional help should be sought).

Guidelines

Informal Guidelines

1. Is there something you or others would prefer to keep quiet?

Are there "shushers" in the situation? Who wants to keep things quiet?

Does it pass the Mom Test: Would you tell her? Would she do it?

Does it pass the TV Test: Would you tell a nationwide audience?

Does it pass the Market Test: Could you advertise the activity to gain a market edge?

2. Does your instinct tell you that something is wrong?

Does it pass the Smell Test: Does the situation "smell"?

Formal Guidelines

1. Does the act violate corporate policy?

2. Does the act violate corporate or professional codes of conduct or ethics?

3. Does the act violate the Golden Rule?

Ethical Principles

Rights and Duties (deontology)

Are any rights abridged?

The right to know

The right to privacy

The right to property

Are any duties or responsibilities not met?

Personal duties:

Trust Integrity Truthfulness Gratitude and reparation

Justice Beneficence and nonmaleficence Self-improvement

Professional duties (responsibilities)

For all professionals:

Maintain appropriate professional relationships

Maintain efficacy

For information professionals in particular:

Maintain confidentiality

Maintain impartiality

Consequentialism (teleology)

Does the action minimize actual and potential harm?

Egoism: good for me, least harm to me

Utilitarianism: good for the group, least harm for the group

Altruism: good for all, some harm to me

Kant's Categorical Imperative

The principle of consistency: What if everyone acted this way?

The principle of respect: Are people treated as ends rather than means?

In the following sections, I illustrate key questions about the ethical dimensions of anonymity and pseudonymity following the Kallman & Grillo approach. For purposes of illustration, the ethical question under discussion is whether a member of the information systems staff of a corporation should post an anonymous message in a Usenet group warning users about a flaw in a competitor's software product.

Law and Ethics

Does the law provide an answer? Is the proposed anonymous message illegal? An attorney or other legal expert would have to be consulted about this question.

Guidelines

The law is never the only determinant of the advisability of an action. We usually incorporate guidelines that have not been codified into law into our moral universe.

Informal Guidelines

Some guidelines are informal -- they are not usually even written down at all.

One class of questions we can use to judge whether informal guidelines support a proposed action or militate against it is represented by the question "Is there something you or others would prefer to keep quiet?" For instance, are there "shushers" in the situation? Are people trying to keep the proposed action quiet? Who are the people who want to keep things quiet and what are their motivations?

Does posting an anonymous warning pass "the Mom Test:" Would you tell your mother? Would she do it? These questions reach deep into the earliest years of ethical training. The response may indicate that something is fundamentally antithetical to one's underlying moral principles -- or that perhaps it's acceptable.

Does it pass the TV Test: Would you tell a nationwide audience? If the gut-level answer is, "No!" there is almost certainly something wrong with the proposal.

Does it pass the Market Test: Could you advertise the activity to gain a market edge? Would people you do business with respect you for having posted an anonymous warning about your competition's product?

Does your instinct tell you that something is wrong? Does it pass the Smell Test: Does the situation "smell"? That is, do you feel an undefined reluctance to act as proposed? If so, it is worth exploring the situation more thoroughly to see if the proposed action fits into the normal framework of acceptable behaviour you have established

Formal Guidelines

Formal guidelines include the written rules of corporate and professional behaviour. Violating these rules may have serious consequences such as termination of employment or expulsion from professional bodies.

The simplest questions are "Does the act violate corporate policy? Does the act violate corporate or professional codes of conduct or ethics?" Discussion of a proposed course of action with colleagues and with managers will generally clarify the situation.

Does the act violate the Golden Rule? This question refers to a principle sometimes expressed as, "Do not do to others what you would not have done to you." For this question to be meaningful, questioners must be able to empathise with others -- to put themselves in other people's place. Although young children cannot accomplish this empathic projection, most adolescents and adults can do so. Sociopaths are defined in part by their inability to conceptualise anyone else's point of view or feelings.

Ethical Principles

How do people make judgements about a course of action when there are no guidelines? There are several kinds of principles that people use in reasoning about a new situation.

Rights and Duties (deontology)

The concepts of rights ("Something that is due to a person or governmental body by law, tradition, or nature. . . .") and duties ("An act or a course of action that is required of one by position, social custom, law, or religion. . . ." -- both definitions from the *American Heritage Dictionary*, 1992) should influence one's decisions.

Are any rights abridged? For example, the right to know the source of a warning so that we may judge the motives and credibility of the statement are infringed when such a message is posted anonymously or pseudonymously.

Personal duties at issue in a decision on posting anonymous warnings about a competitor's product include notions of trust, integrity, and truthfulness, all of which are violated by such an act. We lower the trust of technical advice when we use anonymous postings; we damage the integrity of an entire profession; and we implicitly betray truthfulness by failing to identify the source of such information.

Professional duties or responsibilities also apply. We are expected to maintain appropriate professional relationships, but anonymous posting does not further a web of trust among colleagues. Posting anonymous messages casts doubt on the good will of all the innocent people who are perceived as possibly being the author of such messages. In terms of maintaining efficacy, anonymous postings reduce the flow of information among professionals by aborting the possibility of private communication with the authors of the anonymous messages.

Consequentialism (teleology)

One approach to evaluating the ethical dimensions of a proposed act is to look at the possible consequences of the act. Does the action minimise actual and potential harm? Egoism looks at what is good for me or does the least harm

to me. Anonymous posting of critical information about a competitor's product offers the potential of benefits to one's employer with minimal direct consequences. On the other hand, such behaviour opens up the organisation to less obvious consequences such as the risk of blackmail, degradation of trust within the group, lowered morale, and departure of employees whose moral sensibilities are outraged by what they see as unethical behaviour.

Utilitarianism views decisions in terms of what is good for the group or does the least harm for the group. The question here is the inclusivity of the "group." If the group includes all users and potential users of the defective product, then posting the information serves a good purpose; the decision on whether to post anonymously resolves to the same questions as those raised in discussions of the consequences for an organisation of having an employee post messages anonymously. The climate of trust, the credibility of warnings in general, and respect for the entire industry can be harmed by anonymous postings of warnings.

An altruistic approach to decisions accepts that what is good for all may be worth doing even if there is some harm to me. By this yardstick, posting a warning with full attribution is definitely the preferred way of communicating information about a problem. Another altruistic approach, however, would be to inform the competitor of the flaw in their product via private communications. The hope here is that such altruism will be reciprocated and that the industry as a whole can benefit from improvement in all products.

As a side note, the ICSA's Antivirus Product Developers' Consortium is in a sense based on such altruistic premisses. From the inception of this project, the ICSA (formerly the ICSA) argued that it was counter-productive for antivirus product developers to sequester information about new virus strains. Instead, argued the ICSA, developers should contribute all new virus strains to a "zoo" from which all developers could draw samples to ensure that all ICSA-certified products could identify and combat all specified viruses. Although in the short run some antivirus products might lose a competitive edge, eliminating the element of private knowledge of virus strains would help the consumer and therefore the industry as a whole.

Kant's Categorical Imperative

At a different level, Immanuel Kant's principles for judging the ethical dimensions of an act are immensely useful in all aspects of life. The principle of consistency asks, "What if everyone acted this way?" In our example, if everyone posted anonymous warnings the credibility of all warnings would be damaged. In the absence of a mechanism of redress, unscrupulous people would contaminate the alerts with false information, making it difficult to trust any warning. Since some people would retaliate for fraudulent postings about their products by posting equally fraudulent attacks on their competitors, the system of alerts would collapse, causing harm to users and to producers.

Another principle Kant enunciated was that of respect: Are people treated as ends rather than means? The author of an anonymous message may not be thinking about the people affected by that message; they remain ciphers -- amorphous, unknown entities of no importance. In contrast, an empathic and ethical person remembers that every group consists of individual human beings with pretty much the same range of feelings as anyone else. Using them as a means of increasing market share is not respectful.

6.3 Corporations and other organisations

How can organisations contribute to the reduction of harmful anonymous or pseudonymous communications?

Every corporation, government department, non-profit organisation, educational institution, health-care facility, banking or financial services organisation and so on should explicitly address the question of anonymity and forgery on the Net. The following are some practical guidelines to consider in setting organisational policy:

No user of a corporate user ID should ever forge headers or use pseudonyms when communicating using corporate resources.

Corporate firewalls should be configured to prevent all TCP/IP packets from passing outward through the firewall with forged IP addresses.

SMTP servers should be configured to prevent any e-mail from leaving a site with forged headers.

All corporate e-mail outbound from a site should be signed digitally by its author(s) to provide a basis, when

necessary, for repudiation of unsigned and fraudulent e-mail.

In addition, discussions of the ethical framework for making decisions about the use of technology should be integrated into employee training at all levels. Managers, in particular, ought to be cognisant of the principles of ethical decision-making so that they can fluently guide their staff in practical problem-solving.

6.4 Internet service providers

Because many users send e-mail or post to Usenet groups through accounts with ISPs, these services have an obligation to become involved in preventing abuses of anonymity and pseudonymity. Except for some free services who are independently funded or who derive revenue from advertising rather than from user fees, ISPs must establish a relationship with their users to be paid; most use credit-card accounts as their means of being paid. This method of billing inherently provides a link to the real-world identity of a user through the credit-card issuers. Thus for most ISPs, it is possible to enforce *traceable* anonymity and pseudonymity. Faced with a subpoena, for example, most ISPs will be able to provide authorities with all the information needed to track down the person whose account was used to send a message. Whether the owner of the account is the author of a particular message depends on the security of identification and authentication mechanisms in use. Passwords, for example, are unlikely to be considered strong authentication because there are too many ways passwords can be compromised. Biometric authentication, on the other hand, may provide for strong authentication if error rates are considered sufficiently low to warrant the imputation of authorship based on biometrics.

One of the most interesting suggestions about the role of ISPs in governing anonymity and pseudonymity -- and behaviour in general -- in cyberspace comes from Lewis (1996). Lewis suggested that those interested in banning anonymity online could support ISPs requiring traceable identity for all their customers. Let individuals choose what kind of ISP they want to use, but control access to their communications according to the degree of strong identification and authentication in use by the ISP. This suggestion is remarkably close to Post & Johnson's (1997) work on model systems in that ISPs can play a pivotal role in determining the future of the Internet without having to involve governments.

Some practical suggestions for ISPs:

ISPs should automatically sign every outbound message using their Public Key Cryptosystem secret key (PGP 1997; RSADSI 1997).

Every e-mail message could instantly be verified as authentically coming from the specified ISP; forgeries would be practically impossible as long as the security of the ISPs secret keys was maintained.

The next step would be publication of every ISP's terms of service in a public forum, signed by its secret key; these summaries would immediately allow ISPs to sort themselves out according to how restrictive their policies on anonymity and pseudonymity were.

The SMTP would have to be modified to provide for verification of digital signatures, but given such changes, any ISP could automatically block incoming mail from ISPs whose policies were unacceptable.

For example, suppose the Truthful ISP insisted on maintaining records of exactly who was registered for any given ID and blocked outbound forged e-mail and unsolicited commercial e-mail. Truthful ISP might want to block mail from the CyberSleaze ISP where forgeries and floods of spam were commonplace.

What might happen over time as this practice of allowing communications only with selected ISPs as a function of their terms of service? Eventually there would likely be an equilibrium in which those users who wished to send and receive anonymous, untraceable e-mail could subscribe to those ISPs supporting that kind of communication. Others could automatically block e-mail from unwanted ISPs. Furthermore, individuals who wished to use anonymity or pseudonymity sometimes could subscribe to more than one ISP and take advantage of their different policies. The computer systems manager who wanted to deal only with other professionals at work could use a restrictive ISP; however, she could also use a different ISP to post and read messages in a highly-charged, free-wheeling discussion group about the politics of gun control without having to reveal her real name or fearing that she could ultimately be traced through a pseudonym.

As the forces of the marketplace continued to work on ISPs, there might be further evolution towards different degrees and types of blockage of communication. ISPs with a reputation for harbouring miscreants who libel and defame others without cause could find themselves being shut out of an increasing number of reputable communities of users. Those whose users exercised moderation and responsibility might find themselves being received by a widening circle of ISPs.

The advantage of this model is that individuals could exert power over their electronic environment by voting with their subscriptions, but no one would be censored by bureaucrats or tyrants. Just as Hyde Park in England allows both geniuses and crackpots to speak, yet forces no one to listen, the electronic Hyde Park would provide a mechanism for shutting out the lunatics all the while letting the loonies talk to each other as they wish.

What this model would not permit is the imposition of unwanted communications on powerless victims. This model would spell the end of unsolicited commercial e-mail. If digital signatures indicating the source ISP from which executable code were first distributed became commonplace, the same mechanism could seriously interfere with the distribution of viruses and other harmful programs. ISPs that became known for harbouring virus-writers or -distributors would see their credibility as communications partners eroded. Note that this model does not require the individual to sign his or her product or message; the only constraint is that the ISP do so.

What about individuals who own their own domain on the Net? The same principles would apply. The modified SMTP software would automatically sign all output from their sites. Any site that refused to provide digital signatures could be excluded by any ISP that chose to apply such an exclusionary rule.

6.5 Governments

The role of governments in cyberspace is complex. On the one hand, several governments -- notably that of the United States -- have contributed to the development of the Internet through legislation and funding. On the other hand, many governments, especially totalitarian regimes, are intolerant of unfettered communications. Under the Communist regimes, most countries in the USSR and its satellites made ownership of unregistered spirit duplicators, photocopiers, fax machines and modems illegal. Today, Burma, in the grip of the tyrannical State Law and Order Restoration Committee, still does.

In recent months, there have been several moves to restrict access to the Internet or to control access to content from the Net around the world. Although there are no specific governmental efforts listed to control anonymity and pseudonymity, the following review of legal and legislative developments from 1997 alone will illustrate the wide range of usually unsuccessful efforts to extend the rule of law to cyberspace (Kabay, 1997):

China marginally relaxed its restrictions on Internet access, but it continued to block sites that report news from Hong Kong and Taiwan.

The German government filed charges against Angela Marquardt, the deputy leader of the communist Party of Democratic Socialism, for linking from her Web page to a banned issue magazine called *Radikal*. The issue of *Radikal* was banned because it included detailed instructions on how to sabotage railway lines. According to the public prosecutor, "It has nothing to do with censorship. Criminally relevant materials are subject to classification by the district attorney or criminal prosecutors." In early June, the court hearing opened and adjourned after an hour so the magistrates could arrange for expert testimony to explain the Net and the Web when the case reconvened toward the end of June. On June 30, the court ruled that maintaining a hyperlink to objectionable material is not tantamount to publication of that material.

New York's online-decency law barring computer-based distribution of indecent materials harmful to minors was challenged by the ACLU and 14 other organisations. The ACLU argued that New York's law "does not define the relevant 'community' for purposes of determining what is 'patently offensive' in the global medium of cyberspace," nor does it distinguish between what might be harmful to young children and vs. what might be harmful to teenagers. Finally, the lawsuit said the statute violates the Commerce Clause because it attempts to regulate communications that take place outside New York, poses an unreasonable burden on interstate and foreign commerce, and subjects interstate use of the Internet to inconsistent regulations. The ACLU won the case in June, resulting in a ban on enforcement of the NY law pending appeal to the Supreme Court of the United States.

The US Department of Justice prepared to support the Communications Decency Act by claiming that because families and children use the Internet, therefore the CDA is not an infringement of the First Amendment to the US Constitution (guaranteeing free speech).

The United Arab Emirate's government-controlled ISP has set up a proxy server to censor the Net. The country's 9,669 Etisalat users are required by law to configure their Web browsers to use the official proxy server that filters out offensive materials.

An editorial in the Iraqi government newspaper Al-Jumhuriya says that the Internet -- which is not accessible in Iraq -- is "the end of civilisations, cultures, interests, and ethics," and "one of the American means to enter every house in the world. They want to become the only source for controlling human beings in the new electronic village."

A Maryland bill that would make it illegal to send "annoying" or "embarrassing" e-mail was introduced in early February by Democratic General Assembly member Samuel Rosenberg. Critics describe the proposed legislation as using impossibly vague terms and being unconstitutional."

Not everyone supports calls for freedom of speech and absence of government controls on the Net. At the World Economic Forum in Switzerland, representatives from such countries as Iran called the pressure for unfettered communications an ideology and explicitly rejected liberalism.

The British government announced that it may introduce legislation to interfere with neo-Nazi use of the Internet.

Vietnam joined the growing roster of authoritarian regimes scared into needing laxatives by the prospect of allowing their citizens to read whatever they want.

A new law proposed in Sweden would guarantee free speech rights to people publishing non-modifiable texts on the Internet provided that a named person be the "responsible editor" who would have legal responsibility for the texts being posted.

The Bavarian state prosecutor's office laid criminal charges in April against Felix Somm, head of CompuServe Germany. The indictment cites the online availability of "images of child pornography, violent sex and sex with animals" through CompuServe's making the USENET available to its users. CompuServe vowed to support its employee in the case. An interesting development occurred in June, when the federal parliament began consideration of the Information and Communications Services Law, which would exempt carriers and ISPs from prosecution for the content of their traffic."

The ACLU threatened to launch court actions against the Ohio Public Library Information Network because state librarians decided to install Net filters to stop kids from surfing through pornographic and other undesirable sites. Undesirable by others than the children, that is. The fuss began when six boys in a county library were discovered to be gawking at pornographic pictures from the Internet. A month after the ACLU's intervention, a parents' group, Citizens for the Protection of Children, vigorously supported the proposed filters.

In Virginia, state employees such as professors at state-funded universities and colleges are forbidden to view sexually explicit online materials. Six Virginia university professors and the ACLU filed a challenge to the legislation, which interferes with online access to materials that are available on paper without question. Currently, it is "a crime for state employees using state-owned computers to `access, download, print or store any information . . . having sexually explicit content.'" The law also seems to apply to non-pornographic but sexually-explicit information such as the classic English poetry of Swinburne or the historically important works of Sigmund Freud. The federal lawsuit demands that this state law be overturned. The plaintiffs say this is insulting and a breach of academic freedom.

Two self-described worshippers of Satan launched a lawsuit against ElectriCiti Inc., a San Diego ISP, for failing to shut down one of their persistent anonymous public critics. The ISP's lawyers countered that the short-lived Communications Decency Act precluded suing ISPs for the content of messages posted on the Net. In addition, the defendants claimed that the lawsuit by Michael and Lilith Aquino is a "SLAPP" C "strategic lawsuit against public participation" and should be dismissed out of hand.

In a Federal Circuit court in Florida, Judge James Carlisle ruled in June that AOL is not liable for the content of cyberchat. The case concerned a civil lawsuit by the parents of a 14-year-old boy who was raped by Richard Lee Russell in 1994 after the two met in an AOL chat room. The parents said they would appeal the ruling.

The White House back-pedalled on its support for the notorious Communications Decency Act, apparently anticipating the Supreme Court's rejection of this law's constitutionality. Observers chuckled over the abrupt reversal from the Department of Justice's position in March, when the administration vigorously asserted the value of this law.

In a case brought by the ACLU, US District Judge Loretta Preska issued a temporary injunction in June preventing prosecutions under New York State's new law making it a criminal offence for paedophiles to use the Net to entrap children. The Judge wrote, "The protection of children from paedophile is an entirely valid and laudable goal of state legislation. The New York act's attempts to effectuate that goal, however, fall afoul of the (federal) Commerce Clause." In a similar case in Georgia, Senior US District Judge Marvin Shoob of the Atlanta federal court ruled that the Georgia law making it illegal to use pseudonyms on the Net was subject to challenge by the ACLU and others and suspended enforcement pending resolution of the lawsuit."

China passed even more draconian laws restricting access to the Internet by its citizens. The regulations force all Net access to go through the government's proxy servers to permit extensive censorship.

In a stinging rebuke to censorship buffs in the US, the Supreme Court issued its ruling on the Communications Decency Act, finding that it violated First Amendment protection of free speech. The unanimous opinion stated that the effort to protect children from sexually explicit material goes too far because it also would keep such material from adults who have a right to see it. Justice John Paul Stevens wrote for the court, "The (Communications Decency Act) is a content-based regulation of speech. The vagueness of such a regulation raises special First Amendment concerns because of its obvious chilling effect on free speech. . . . As a matter of constitutional tradition . . . we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it." See http://www.cdt.org or http://www.epic.org for the full text of the ruling, which was noteworthy for the clarity of its prose and spirited defence of free speech on the Net.

In the wake of the CDA decision by the Supreme Court of the US, European Internet experts warned that no country should try to "change the Internet we know and love into a kindergarten." Regulating the Internet would in any case require extensive international co-operation because of the international nature of the Net.

The American Library Association's Intellectual Freedom Committee issued a statement on the problems faced by libraries in using Internet-filtering software. The report pointed to the Supreme Court ruling of 1997.06.29 on the Communications Decency Act affirming the protected status of speech on the Internet. In addition, said the ALA statement's authors, libraries must serve a wide range of users; filtering software is generally designed for families or corporations where centralised controls can successfully be dictated for children or employees. Filtering software imposes unreasonable restrictions on everyone to protect a minority of users; "can impose the producer's viewpoint on the community;" does not "generally reveal what is being blocked, or provide methods for users to reach sites that were inadvertently blocked;" and use "vaguely defined and subjectively applied" criteria for blocking sites.

The German federal legislature passed a law to prosecute Internet Service Providers that make illegal materials available on-line; e.g., child pornography or Nazi publications. Commentators scoffed that the law was too vague for enforcement and could not be made to apply to international networks. In other developments, government representatives from Canada, Europe, Japan, Russia and the US met in Bonn with officials from ISPs to sort out the issue of regulation and prevent hobbling the new mode of communication.

Another farcical situation was revealed when three counties in New Jersey discovered that their sites are blocked by the notorious AOL "Scunthorpe" filter. All the sites included the three letters "sex" in their names.

The Australian government proposed new laws under the Broadcasting Services Act to make ISPs liable for criminal breaches of the regulations of the Office of Film and Literature Classification and other laws. The Australian Industry Association hailed the proposals as "a sensible balance between community concerns over Internet content and business concerns on over-regulation." Communications Minister Richard Alston stated that the government realises that it cannot regulate the global Internet, but said the government will help control access by minors so that

parents and guardians can prevent abuse.

Members of the Library Board in Loudon County, VA voted 6-2 to install filtering software on their Internet terminals and to ask adults to request inactivation of the filters when desired. Children aged 16 and younger will have unfettered access to the Internet from Library terminals only when their parents are with them.

According to the Investor's Business Daily, the recent deal between tobacco companies and many states would prohibit tobacco advertising on the Internet. Commentators worry that this precedent could cripple online speech from international companies by enforcing the most restrictive laws found anywhere around the world.

The Yemeni government suspended cellular phone services to 9,000 residents because of security concerns. The authoritarian government has been fighting a resurgence of terrorism in the country and unfettered communication is clearly seen as a threat to its power.

Communications Minister Richard Alston announced that the Australian Broadcasting Authority would begin discussions with ISPs to establish new codes of practice to prevent distribution of offensive materials through the Internet.

In the United Arab Emirates, hackers are more interested in evading clumsy government attempts to limit access to the Internet than in invading other people's computer systems. Savvy users have been side-stepping government restrictions to access pornography and C even worse C to talk to Israelis. In Saudi Arabia, fear of the Net has prevented any local ISP from being set up, but rich users simply place international long-distance calls to external ISPs.

The Pennsylvania legislature unanimously passed a law criminalizing the use of the Internet to lure children or teens into sex acts.

New York Penal Law 235.22 criminalizes the distribution of indecent material online to minors that is for the specific purpose of inducing them to engage in sexual acts. This law, to take effect 1 Nov 96, has gained the support of free speech advocates and opponents of child pornography alike. It was successfully upheld in the case of People v. Barrows, Justice Alan Marrus of the New York State Supreme Court presiding. He ruled for the first time to uphold an indictment under the luring statute. The case involved a 56-year-old man who is alleged to have tried to lure a 13-year old virtual girl into a meeting C and arrived equipped with a rope, lubricants and paper towels. He was arrested by a female police officer posing as the child. His attorney protested the grand jury indictment on free speech grounds but lost because, ruled the judge, the element of luring overshadowed speech issues.

In October, the Canadian Human Rights Tribunal began an interesting hearing into the possibility of limiting the publication of the writings of notorious Holocaust-denier Ernst Zundel on a Web page physically located in California. EFF Canada President, David Jones of McMaster University warned that the law in question was written to handle hate-messages on phone-answering machines and suggests that extending it to deal with the Internet ought to be subject to wide public debate. In an editorial, the Globe & Mail came down, as usual, strongly in favour of free speech. Marginal and delusional cases like Zundel don't deserve the publicity they garner through legal prosecution.

No matter how carefully crafted they are, attempts to apply legal constraints on anonymity in cyberspace will be undermined by inconsistent government regimes throughout the globe. The least restrictive geographical entities will subvert more restrictive jurisdictions (Froomkin, 1995). If, say, Restrictopolis were to impose strictures on anonymous Internet use, its anonymity-seeking citizens might be able to use the ISPs in Liberalopolis, where the rules would be much more free.

On a less practical, more philosophic level, there are profound objections to any government regulation of the Internet. As Lewis (1996) writes,

"We do not outlaw wig shops or Halloween masks just because some people use them for illegal or immoral purposes. We do not require caller-ID services for everyone just because some people make obscene or harassing phone calls. Nor should we strip the cloak of online anonymity from everyone, including those who legitimately need privacy, just to prevent sickos from abusing it."

In the United States, the government would likely run up against strong constitutional guarantees of speech, especially political speech -- and including anonymous political speech -- if it tried to ban anonymity outright (Lessig et al. 1997b).

A particularly significant setback for government attempts to control anonymity in the US came in June 1997. The case began in January 1997 (McCullagh, 1997a). As Declan McCullagh (1997b) described the judgement,

"In Georgia, Judge Marvin Shoob ruled that a state law forbidding anonymity online is unconstitutional since it violates free speech and free association rights. The law is so broadly written, the judge indicated, that even America Online screen names could be considered illegal. . . . Judge Shoob "understood clearly the very strong need for our plaintiffs to communicate anonymously," the ACLU's Ann Beeson says. Both judges [in Georgia and in a similar case in New York] issued preliminary injunctions barring the state attorneys general from enforcing the laws. . . .

Georgia's Judge Shoob, in a . . . 21-page opinion, ruled that the law -- that the Democrat-controlled legislature passed in haste last year to muzzle a dissident Republican representative -- violated the First Amendment.

This echoes a recent Supreme Court case, McIntyre v. Ohio, in which the justices ruled that the right to anonymity extends beyond political speech; that requiring someone to add their name to a leaflet is unconstitutional; that writing can be more effective if the speaker's identity is unknown."

In my opinion, governments world-wide would do better to stay out of cyberspace and allow users to develop their own transnational solutions for governing behaviour, including the use of anonymity and pseudonymity.

7 Concluding remarks

I hope that readers of this brief review of anonymity and pseudonymity will take away the following key points:

Anonymous and pseudonymous communications are inherently associated with an increased incidence of antisocial behaviour through *deindividuation.*

There are circumstances where anonymity and pseudonymity are useful tools in the defence of liberty and justice.

Anonymous and pseudonymous electronic communications have already been used to harass victims, damage commercial interests, and launch hoaxes and rumours into cyberspace.

The major problems of anonymity and pseudonymity in cyberspace can be avoided by the use of *traceable* identification.

Making ISPs responsible for enforcing their chosen level of strong identification and authentication will allow a non-governmental, non-legalistic approach to reducing abuse by anonymous and pseudonymous Internet users.

All electronic communications ought to be tagged with unforgeable authenticators of identity.

Individuals, families and schools have a role to play in integrating cyberspace into the moral universe of children.

Corporations and other organisations ought to integrate ethical decision-making into their management procedures.

Governments will continue to fail in their efforts to govern cyberspace because electronic communications networks are inherently divorced from geographical jurisdictions.

Finally, a new discussion group has recently been established for discussions of anonymity and pseudonymity. For more information, see http://www.well.com/~declan/nym/. To join, send the message "subscribe nym" to majordomo@vorlon.mit.edu.

8 References

Notes:

every reference to a Web document was verified and was valid on January 30, 1998.

**** marks secondary reference drawn from Myers, D. G., 1993; Lippa, R. A., 1994; or Sears, D. O., Peplau, L. A., & Taylor, S. E., 1991.***

American Heritage Dictionary of the English Language, Third Edition, The (1992). Houghton Mifflin Company. Electronic version licensed from InfoSoft International, Inc. and made available in the Windows95 MicroSoft Bookshelf CD-ROM

Anonymous (1996a). "Medusa's Snakes in Cyberspace, a WWW site honoring the notorious and infamous net legend and crackpot extraordinaire, L. Detweiler." Online via http://www.sni.net/~ldetweil/

Anonymous (1996b). History of L. Detweiler. Online via http://www.sni.net/~ldetweil/medusa/detweiler.html

Buford, B. (1991). *Among the thugs*. Mandarin Paperbacks (London). ISBN 0-7493-1328-5. 318 pp

Card, O. S. (1985). *Ender's game*. Tor Books (New York). ISBN 0-812-51911-6

Clarke, R. (1997a). Introduction to dataveillance and information privacy, and definitions of terms. Online via http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html

Clarke, R. (1997b). Human identification in information systems: Management challenges and public policy issues. *Information Technology & People* 7(4):6-37. Online via http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html

Covington, S. (1997). Judgment No. 97-06273 of the District Court of Travis County, Texas, 345th Judicial District. http://www.zilker.net/nospam/judgment.html

Csikszentmihalyi, M. (1990). *Flow: The psychology of optimal experience*. Harper & Row (New York). ISBN 0-06-016253-8

Detweiler, L. (1993). Identity, privacy, and anonymity on the Internet. Online via http://www.intac.com//man/faq/net-privacy/part1

Diener, E. (1979). Deindividuation, self-awareness, and disinhibition. *Journal of Personality and Social Psychology* 37:1160-1171*

Diener, E., Fraser, S.C., Beaman, A. L. & Kelem, R. T. (1976). Effects of deindividuating variables on stealing by Halloween trick-or-treaters. *Journal of Personality and Social Psychology* 33:178- 183.*

Elman, A. (1997). College web surveys hazardous to your server's health. RISKS Forum Digest 19(46). Available online at http://catless.ncl.ac.uk/Risks/19.46.html

Festinger, L., Pepitone, A. & Newcomb, T. (1952). Some consequences of deindividuation in a group. *Journal of Abnormal and Social Psychology* 47:382-389*

Free, C. (1997). Make their day: fury at the wheel turns frustrated drivers into outlay Dirty Harrys with a rage for revenge. *People Weekly*, 48(9):59

Froomkin, A. M. (1995). Anonymity and its enmities . *J. Online Law*, article 4 http://www.law.cornell.edu/jol/froomkin.htm

Froomkin, A. M. (1996) Flood control on the information ocean: Living with anonymity, digital cash and distributed databases. *U. Pittsburgh Journal of Law and Commerce* 15:395. Online via http://www.law.miami.edu/~froomkin/articles/ocean1.htm

Gergen, K. J., Gergen, M. M., & Barton, W. H. (1973). Deviance in the dark. *Psychology Today* (October):129-130*

Johnson, C. (1995). Anonymity on-line? It depends on who's asking. *The Wall Street Journal*, Nov 24, 1995 p.B1 col 3

Kabay, M. E. (1994). Totem and Taboo: Civility and Vandalism in Cyberspace. *Proceedings* of the 17th National Computer Security Symposium, Baltimore, MD (Oct 11-14, 1994). Reprinted in *ICSA News* (June 1995):4. Online via http://www.icsa.net/library/g.html

Kabay, M. E. (1996). The InfoSec year in review 1996. http://www.icsa.net/library/isecyir.html

Kabay, M. E. (1997). The InfoSec year in review 1997. http://www.icsa.net/library/iyir.html

Kauffman, S. A. (1993). *The origins of order: Self-organisation and selection in evolution.* Oxford University Press (Oxford, UK). ISBN 0-19-507951-5.

Kallman, E. A. & J. P. Grillo (1996). *Ethical decision making and information technology: An introduction with cases, second edition.* ISBN 0-07-034090-0.

Kerr, J. H. (1994). *Understanding soccer hooliganism.* Open University Press (Buckingham). ISBN 0-335-19249-1*

Le Bon, G. (1896). *The crowd: A study of the popular mind.* Macmillan (New York)*

Lessig, L., Post, D., and Volokh, E. (1997a). *Cyberspace law for non-lawyers.* Lesson 23 -- Privacy 11: Privacy: Self-Help: Anonymity, Part 1. Online via http://www.ssrn.com/update/lsn/cyberspace/lessons/priv11.html

Lessig, L., Post, D., and Volokh, E. (1997b). *Cyberspace law for non-lawyers.* Lesson 24 -- Privacy 12: Privacy: Self-Help: Anonymity, Part 2. Online via http://www.ssrn.com/update/lsn/cyberspace/lessons/priv12.html

Lewis, P. (1996). Cloaks and daggers: Online anonymity is a blessing and a curse. *Home Office Computing* 14(7):133

Lippa, R. A. (1994). *Introduction to social psychology, second edition.* Brooks/Cole Publishing (Pacific Grove, CA). ISBN 0-534-17388-8

McCullagh, D. (1997a). Brick by brick. The Netly News (Editorial). Online via http://cgi.pathfinder.com/netly/editorial/0,1012,590,00.html

McCullagh, D. (1997b). Courts strike down New York and Georgia Net-censorship laws. Sent Fri, 20 Jun 1997 13:49:06 -0700 (PDT) on fight-censorship-announce@vorlon.mit.edu mailing list.

Myers, D. G. (1993). *Social psychology, fourth edition.* McGraw-Hill (New York). ISBN 0-07-044292-4

Pappas, C. (1997). The A to Z of Internet sleaze. *Home Office Computing* 15(8):70

PGP (1997). Introduction to Message Privacy. Online via http://www.pgp.com/privacy/intro-priv.cgi

Post, D. & Johnson, D. R. (1997). The new civic virtue of the Net: Lessons from models of complex systems. Online via http://www.cli.org/paper4.htm

Post, D. (1995). Knock knock, who's there?: Anonymity and pseudonymity in cyberspace. Online via http://www.cli.org/DPost/X0012_KNOCK.html

Prentice-Dunn, S. & Rogers, R. W. (1980). Effects of deindividuating situation cues and aggressive models on subjective deindividuation and aggression. *Journal of Personality and Social Psychology* 39:104-113*

Rose, L. J. (1994). *NetLaw: Your rights in the online world.* Osborne/McGraw-Hill (New York). ISBN 0-07-882077-4. Pp. 183-4

RSADSI (1997). Frequently Asked Questions: Cryptography -- The Latest from RSA Labs. Online via http://www.rsa.com/rsalabs/LABSFAQ.PDF or ftp://ftp.rsa.com/pub/pdfs/LABSFAQ.PDF

Russell, J. J. (1997). The new menace on the road. *Good Housekeeping* 224(4):100-10

Sears, D. O., Peplau, L. A., & Taylor, S. E. (1991). *Social psychology, seventh edition.* Prentice-Hall (Englewood Cliffs, NJ). ISBN 0-13-817099-1

Spivey, C. B. & Prentice-Dunn, S. (1990). Assessing the directionality of deindividuation: Effects of deindividuation, modeling, and private self-consciousness on aggressive and prosocial responses. *Basic and Applied Social Psychology* 11:387-403*

Ubois, J. (1995). Anonymity has its place. *MIDRANGE Systems* 8(8):28

Watson, R. I. Jr (1973). Investigation into deindividuation using a cross-cultural survey technique. *Journal of Personality and Social Psychology* 25:342-345*

Winton, N. (1997). Unstoppable Internet will defy controls. Reuters World Report (January 16, 1997 21:37:00 GMT)

Zimbardo, P. G. (1970). The human choice: individuation, reason and order versus deindividuation, impulse, and chaos. In Arnold, W. J. & D. Levine, eds (1969). *Nebraska Symposium on Motivation.* University of Nebraska Press (Lincoln)*

About the Author

Mich Kabay began programming computers in 1965. After completing a BSc with concentration in Genetics (1970) and an MSc in teratology (1972) from McGill University, he received his PhD from Dartmouth College in applied statistics and invertebrate zoology in 1976 and taught as a university professor in Canada and abroad. He switched to computer science in 1979, when he helped write a compiler for a 4GL and RDBMS. From 1980 to 1984 he was an operating system internals and performance specialist for the HP3000 line with Hewlett-Packard in Montreal. He followed this with a couple of years as operations manager in a large computer service bureau. Since 1986, Kabay has specialised in consulting and training for systems performance, systems operations, and systems security. He has written security columns for Computer World, Network World, Computing Canada, Secure Computing Magazine, ICSA News, and several other trade magazines. He teaches courses in Information Security & Ethics, Strategic Applications of Information Technology, Data Communications, Quality Assurance, The Art of Technical Support and Information Technology Security. Dr Kabay has published over 170 technical papers and has completed a college textbook, The ICSA Guide to Enterprise Security, published by McGraw-Hill in April 1996. He won the Best Paper Award at the 16th National Computer Security Conference in 1993 for his submission, Social Psychology and INFOSEC: Psycho-social Factors in the Implementation of Information Security Policy. He became the volunteer Director of Education of the National Computer Security Association (now the ICSA) in 1991 and was put on full retainer in that position in 1995. He remains President of JINBU Corporation.

Mailing address: JINBU Corporation, 17 Merineau, Kirkland, QC H9J 3V7 Canada; Phone: (514) 695-4968; Fax: (514) 695-7393; E-mail: mkabay@icsa.net

Descriptors

anti-social behaviour, communications, computing management, defamation, freedom of speech, hoaxes, hostile code, identity, law of cyberspace, libel, privacy, Internet policy

Page content updated March, 1998, by webmaster@icsa.net and published by webmaster@icsa.net