COMPUTERIZED CONFERENCING & COMMUNICATIONS CENTER

at

NEW JERSEY INSTITUTE OF TECHNOLOGY

A Discussion of Selected Aspects of
Privacy, Confidentiality, and Anonymity
in Computerized Conferencing

by

Robert Bezilla

August 1978

Research Report Number Eleven

Computerized Conferencing and Communications Center

c/o Computer & Information Science Department
New Jersey Institute of Technology
323 High Street, Newark, N. J. 07102

A Discussion of Selected Aspects of Privacy, Confidentiality, and Anonymity in Computerized Conferencing

by

Robert Bezilla

August 1978

Research Report Number Eleven

Computerized Conferencing and Communications Center

New Jersey Institue of Technology
323 High St.
Newark, N.J. 07102

Robert Bezilla is Executive Vice President of Benson & Benson, Inc., Princeton, New Jersey. He is an Associate of the Computerized Conferencing and Communications Center at the New Jersey Institute of Technology.

TABLE OF CONTENTS Page

TABLE OF CONTENTS (Cont)

ACKNOWLEDGMENTS

Later in this report there is a discussion of the manner in which computerized conferencing can be employed to provide proper attribution to individuals for group enterprises. Unfortunately, such techniques are still in development and so I must rely upon more conventional means to acknowledge the considerable assistance I have received.

Elaine Kerr, not only cajoled me into exploring and utilizing computerized conferencing in greater depth, but provided invaluable, substantive editorial guidance for this report.

Murray Turoff, Roxanne Hiltz, Barry Wellman, Charlton Price, and Jim Williams were unending sources of ideas, suggestions and encouragement.

And there have been many others, including some, who to my great glee, could be identified only through "anonymous" or pen name designations.

I have been privileged to have learned much from these people, but I must bear the responsibility for whatever syntheses and interpretations I have derived from our discussions, and most especially, I must acknowledge that some of my thoughts have been presented in contradiction of what probably was very good advice.

INTRODUCTION

This paper presents a discussion of the potential uses of privacy, confidentiality and anonymity in computerized conferencing.

Section I begins with definitions of the concepts, their aspects and allied terms; and briefly discusses their use in general communications and problem-solving activities.

Section II explores their use in social research, particularly the survey method, a field that may yield useful analogues for computerized conferencing.

Section III outlines the various functions of privacy, confidentiality and anonymity that have been proposed for their constructive use in computerized conferencing.

Section IV reports various difficulties and compromises that have been encountered to date in striving to achieve true privacy, confidentiality or anonymity in computerized conferencing.

Section V gives preliminary estimates of various ways of enhancing the concepts through computerized conferencing.

SECTION I: Background

The inner thoughts of sentient beings are held in privacy until such time as they may be shared with others. The dissemination of private thoughts to others can be constrained by conditions of confidentiality or anonymity.

In this report privacy is defined as the thoughts, emotions and actions that an individual does not share with others. Confidentiality constitutes the sharing of thoughts, emotions or actions with another party, who may also be given authority to share their content but not the identity of their originator. Anonymity consists of sharing of thoughts, emotions or actions, but with concealment or lack of identification of their perpetrator. When the constraints imposed by confidentiality or anonymity are removed, matters are no longer considered to be private but to enter into the public domain.*

The surrendering of privacy can be said to be either active or passive. Actively, a person may choose to divulge private matters to another, either because that person needs them for some purpose, or to meet some needs of their owner. Passively, social organizations, ranging from dyads to international organizations, may require knowledge of private matters to promote the common welfare; that is, to

---

*A fuller description of the principal terms, their origins, and their current usage in computerized conferencing nomenclature, appears in Appendix A.

protect the rights of a group against the individual or to guide the progress of the group through better knowledge. Frequently, the surrender of one's rights to privacy may be accompanied by stated or implicit guarantees of confidentiality or anonymity.

At its most basic level the right of confidentiality has been recognized historically in such one-on-one relationships as physician-patient, attorney-client and priest-confesser. Violation of these relationships is at the heart of the codes of ethics of these followings and others, and societal sanctions frequently exist against those who would violate or in any way compromise the relationships. Compromise of the privileges usually may be sanctioned only under the direst circumstances, e.g., identification of the bearer of a serious infectious disease. The rights of the individual vs. society are less clear in cases such as the confession of a criminal act. In such cases both a profession and the society in which it functions may claim jurisdiction over the determination of the disclosure of matters given in confidence, and the affected person on occasion can be expected to assert rights of privacy in litigation against the professional or agency if compromises are made. Indeed, the degree and manner of the determination of private rights vs. societal rights can be an important distinguishing attribute of societies, e.g., the "Bill of Rights" of the United States vs. the "collective rights" of the People's Republic of China.

For most everyday societal activities, particularly those related to finance and commerce, privileges of confidentiality are extended rarely except in such sanctuaries as Swiss banks. Consumers frequently are chagrined to discover that their financial affairs, or even personal affairs, may be an open book to tax collectors, creditors, insurers, potential employers and others. In recent years computerized data banks have created means through which much information can be shared and interrelated quickly and efficiently by inquisitive parties. Frequently legislation and regulations do not appear so much to restrict the dissemination of "confidential" files as to set limitations upon the compilation of dossiers through data base interfacing, and, most curiously, to assert the rights of citizens to examine what is known or has been said about them. But even such basic rights would appear to be compromised as disclosures of interagency cooperation are made with disturbing frequency, and as those who go to the trouble to examine files, are dismayed to discover that information about themselves may be withheld from their view on grounds of "security."

Historically, there has been little resistance shown towards releasing aggregated or anecdotal data as long as the individual is not cited as its source; i.e., that the individual's confidentiality is preserved. The American Statistical Association's Ad Hoc Committee on Privacy and Confidentiality asserted recently (1977) that,

> "...of preeminent importance...is the need for achieving a balance between a person's fundamental right to privacy and society's need to acquire information for identification and measurement of its current dimensions and characteristics."

In other words, the aggregate or anecdotal experience of the physician can be recognized as an essential ingredient of diagnostic skill; the attorney's experience contributes to the foundation of legal precedent; and accumulated confidential confessions undoubtedly inspire innumerable sermons. Consumers and their advocates are not likely to be upset by a bank's marketing research that designates average transaction size, by empirically-based actuarial tables, or by census reports derived from aggregated income tax compilations.

The confidential anecdote has been institutionalized as the case history method in many professions, and the aggregation of confidential data is cited as a prime constituent of the nature of statistics by the Ad Hoc Committee on Privacy and Confidentiality.

> "The individual identification of a statistical record and its contents is held confidential from all except the persons collecting and compiling the aggregated data. An individual's record is not used to determine any action that affects the individual except through the contribution of the record to statistical aggregates, averages, or measures of relationships. The very essence of statistical analysis is that the identity of individual units of which it is composed is immaterial. Individuals should not be identifiable in the output of a statistical system."

The nature and constraints governing privacy and confidentiality are at least partially understood by the average citizen, and are tolerated or encouraged by all

governments. Only in the most extreme cases of political imprisonment has their total suppression been attempted. The rights of an entire people probably have never been suppressed uniformly except in the writings on "thought control" by science fiction and fantasy writers. Indeed, Merton (1957) asserts that without opportunities for privacy and confidentiality, the social structure itself would be threatened,

> "Otherwise, the pressure to live up to the details of all (and often conflicting) social norms would become literally unbearable...'Privacy' is not merely a personal predilection; it is an important functional requirement for the effective operation of social structure. Social systems must provide for some appropriate measure, as they say in France, of quant-a-soi -- a portion of the self which is kept immune from social surveillance."

The use of anonymous communication is less frequently made and understood. Totalitarian governments may justifiably regard an anonymous slogan painted on the wall or anonymous pamphlet as a threat to their very existence. In more democratic societies sanctions usually will be invoked against anonymity only in cases of extreme deviant behavior, e.g., threatening letters or obscene telephone calls. Until recently the use of anonymous communication probably has been confined largely to communications by the elite who for various reasons chose to write letters to the editor unsigned or signed with a pen name, authored books under a nom de plume, or contributed to worthy causes as an "anonymous donor" or "friend." Even governments will request

the attribution of remarks to a "usually reliable source" in the free press, or under a fictitious signature in a state-controlled newspaper or journal. It may even be questionable if many such communications are intended to be truly anonymous: the cognoscenti may recognize an old friend behind the pen name, only the very naive would believe that a "citizen" would dare to write a stinging letter of rebuke to a totalitarian state's captive press, and pathological killers have been known to plead anonymously for someone to "stop me before I kill again."

Among non-elites anonymous expression seldom appears to have been available except under bizarre conditions such as the suspension of conventions and physical masking during fertility rites, e.g., modern Mardi Gras celebrations. More recently, however, the introduction of citizen's band radio has captured the popular imagination and the air waves are filled with the fanciful "handles" employed by users to mask their true identities [1]. Celebrities, however, seem to take pains to disclose their CB pseudonyms so that the ordinary citizen will know in reality "First Mama" is the President's wife.

The structured use of anonymity is likely to be encountered only in the work of the research scientist or practitioner. In the social sciences, and particularly in the use of survey research, conditions can exist in which it is desirable to grant and ensure anonymity to research participants who are reporting upon their behavior or ideas;

that is, upon conditions that normally could not be measured accurately without full promise of anonymity. By use of methodologies utilizing anonymous functions, the researcher can promote:

1. Interaction for the free exchange of ideas or the reporting of matters without any threat of disclosure of the same to peers or even to the collectors or compilers of the data; that is, anonymity can remove any threat that the privacy of personal data will be compromised.
2. Objectivity through the masking of identity can serve to suppress distracting sensory cueing or _ad hominem_ fallacies so that the matter being reported or discussed can be considered on its intrinsic merits without regard to personal origins or aspects of origin.
3. Problem solving for the total subordination of the individual ego to the group task. Presumably anonymity can be used to suppress individual considerations that might hinder the group's progress in a mission, e.g., one would not have to worry about peer relations, advancement of unpopular ideas, risk ridicule, etc.

Another form of anonymous function that may be emerging in the physical sciences is that characterized by journalists' pronouncements of the "anonymity" in "Big Science."

Journalists, scientists, students of the social study of science alike have noted for some time a growing trend in the physical sciences that is directing scientific inquiry away from the individual effort towards a necessary joint effort [2]. This development has brought about an approach-avoidance conflict in which scientists recognize an absolute necessity for collaborative effort in certain fields, but equally recognize secondary consequences which make it difficult to reward equitably the contributions of individuals to the group enterprise. The resolution of this dilemma is far from clear, but a possible solution derived from computerized conferencing will be discussed in Section III.

As privacy, confidentiality and anonymity function in a social setting, two further concepts, security and censorship, should be defined for the purposes of this report.

Security is employed in the sense of preserving cognitive space or transmission in such a fashion that unauthorized access cannot be gained casually or sureptitiously, or so that any such attempt will at least be greatly impeded [3].

Censorship constitutes a denial of access to thoughts, communications or information that could be maintained in private, confidential, anonymous or public modes [4].

SECTION II: Social Science and Survey Research Applications

Privacy *per se* is a condition that may be discussed and described by the social scientist, but is of no functional use in scholarship or professional practice because it contradicts the basic scientific requirement to communicate ideas freely with one's peers [5].

Confidentiality, however, is a condition that has long been used by social scientists. In one-on-one relationships, the case histories of individuals revealing their most hidden thoughts, hidden perhaps even to themselves, has been a major foundation of psychoanlytic theory [6]. The confidence established through the client-social worker relationship undoubtedly has established the empirical basis for many social theories that have been derived from the accumulation of multiple experiences. The use of aggregated statistical data, usually collected with assurances of confidentiality, is a hallmark of modern empirical social science. The experimental subject's rights to confidentiality are being spelled out in the codes of ethics of the social science professions and in a set of interlocking federal directives in such detail that many researchers are beginning to worry that their ability to carry out projects may be debilitated [7]. Indeed, even the term "subject" is now seen by many as dehumanizing and as a threat to people's rights. Merton suggests there is an ambivalency in

the need to provide privacy to individuals and to provide also insights to human behavior to social scientists.

> "...the social scientist is so often an object of ambivalence. This is why his inquiries are so often regarded as mere 'snooping' into 'private affairs.' Were it not for other, countervailing mechanisms in society -- such as the institutionalization of 'privileged communications,' or 'data to be treated in utter confidence' -- neither the social scientist dependent upon free access to data on human behavior, nor the other professionals, such as the doctor, lawyer, and clergyman, who must also have this information, would be able to carry out their social roles. But since these social roles are instituionally defined to include unflagging restrictions on making observed departures from the code known to others, the band of observability of deviant behavior can be safely enlarged, without interfering with the functional necessity for 'privacy,' 'secrecy,' or 'ignorance.'"

Methodologies do exist for the granting of anonymity in social science research, but their need and application is comparatively new. Basically, two modes of anonymous protection have been used:

1. Participant anonymity in which experimental subjects are identified to the researcher (who is constrained to hold their identities in confidence), but not to other subjects participating in the experiment.
2. Subject anonymity in which experimental subjects are able to render private information and opinions without revealing their identity to the researcher.

Various social science disciplines have developed means for the protection of anonymity such as the use of masks in psychodramas, but the most systematic means probably have

been used in survey research [8]. In survey research there are four basic methods that have been employed to afford at least operational anonymity to survey respondents.

1. The ballot box technique emulates the anonymity of the election place by allowing respondents to place their completed survey questionnaires in a "secret ballot box." The interviewer does not have access to the individual's opinions or reports because the survey instruments are comingled. The technique also can be employed by allowing respondents to deposit their "votes" [9] through the mail independently so as to deny interviewer access to their reports.
2. Respondent questionnaire selection frequently is combined with the ballot box technique. Respondents can select questionnaires randomly from a stack of questionnaires, or trade questionnaires back and forth so that the data collector has no knowledge of who is filling out which questionnaire. This technique normally forestalls any attempt to identify respondents through sureptitious coding mechanisms [10].
3. Mail surveys can afford a degree of anonymity in that the postmark usually is the only identifying mark. Even postmarks, however, now offer little identity because current postal practices

increasingly call for sectional denotation rather than more specific local or zone names in postal cancellations.

4. A relatively new technique is the use of randomized response which was developed to afford anonymity to respondents in answering questions about such sensitive subjects as drug usage, child abuse, commission of crimes and other deviant forms of social behavior. In this technique a respondent is presented with matching sets of questions on socially-acceptable behavior. The respondent truthfully answers one of the questions, but does not tell the interviewer whether the answer is to the acceptable or to the non-acceptable question. (The respondent chooses the question to be answered through a randomization device such as flipping a coin.) Responses by individual cannot be identified, but the aggregate results can be calculated statistically, and frequently turn out to be higher and more in line with known incidence than those obtained through more conventional methods. To forestall any interviewer interpretation through visual cueing reception, the ballot box or mail survey mode frequently is used in conjunction with this technique [11].

Operationally, all four techniques afford anonymity, but strictly speaking, respondent identity still could be established in most cases through the use of such devices as fingerprint identification or comparisons with previously-known handwriting samples. Use of such extreme uncovering devices is highly unlikely now, but the potential for their use will increase rapidly as such devices as computer-assisted fingerprint identification and optical character recognition become more refined and widespread.

The more common techniques of personal and telephone interviewing afford only confidentiality because interviewers, and frequently questionnaire data compilers, may have access to respondents' names, addresses or telephone numbers. Practically speaking, however, legitimate research organizations institute safeguards to ensure the confidentiality of responses. Additionally, the combination of employee boredom, speed of processing, and sheer numbers is likely to create de facto anonymity; that is; compilers who process thousands of questionnaires a year are unlikely to take the time or the interest to identify individual responses.

Still, the respondent, who rarely is aware of these constraints, is likely, and has every right to insist upon the protection of private data given in confidence in a survey. Misleading devices that intentionally threaten that right can create havoc. Sales organizations, particularly encyclopedia and magazine solicitation firms,

frequently conduct pseudo surveys to exploit the public trust in bona fide surveys for their own ends. Even reputable survey organizations have been known to use ultraviolet ink or other sureptitious means to mark questionnaires for control purposes. Public exposition of this practice has been greeted with outrage, and widespread reforms have been instituted within the survey field to forestall further use of the practice [12]. The practice of some behavioral scientists in using surveys and similar devices to disguise the ulterior objectives of an experiment is receiving closer scrutiny and it has been suggested that such ends do not necessarily justify the means if those means entail potential violation of human rights.

In most forms of survey research, respondents are anonymous to each other, since the only interaction is between the respondent and the interviewer. One form, the focussed group interview, is employed to develop participant interaction to produce cross-fertilization of respondent ideas. A standard practice in forming such groups is to stipulate that respondents have not met prior to the session This affords a degree of operational anonymity in that participants are unlikely to feel that their statements will be identified outside the group by other participants, but peer pressures and visual cueing biases may still be present and vary in degrees of suppression only according to the random personalities of the group and the group

moderator's skills [13].

Delphi technique normally is thought of as a forecasting or problem-solving ("policy delphi") tool, and not as a survey instrument; although it can, and has been used to collect survey data. That it is not used more frequently to collect data is surprising because the technique can feature both participant interaction and participant anonymity [14]. Normally, subject anonymity is not attained in delphi studies because the individual's identity is known to the research compiler, who reiterates the previous response set back to the participant for comparison with the aggregate response. Compiler knowledge of participant identities would be necessary for evaluational and validation studies of the technique, but for conventional application could be circumvented easily with no probable loss to the experiment.

Taxonomically, the delphi method can be viewed as a member of the class of structured group techniques that comprises simulation games and models. A distinguishing characteristic of some members of the class is that many are truly interactive; that is, they are directed by the participants and not by a moderator who is a researcher or a researcher's agent who sets the agenda for the group. Such exercises entail the need of a means of communications and typical examples utilize human referees or computers as referees that assess actions, relay messages, and introduce random events.

As will be discussed later, true interaction could be facilitated by the use of anonymity in computerized conferencing for simulation games and models, and probably extended to researcher-directed activities such as delphi, opinion research and other social research mechanisms.

SECTION III: Applications In Computerized Conferencing

Computerized conferencing could be said to consist of the interactive use of private and shared cognitive space by individuals and by groups.

This space can be structured through programmed or social conventions.

- § Programmed conventions reflect the inherent limitations of the computer hardware chosen for a computerized conferencing system; the extant limitations of supporting software, including languages; and constraints or enhancements purposely introduced in the software package.

- § Social conventions are guided by the constraints imposed by what is possible through use of the available programming; the awareness of the limitations and capabilities for cognitive transmission by members of the computerized conferencing groups; and the development of adaptive social mechanisms by individuals and by groups to compensate for limitations and constraints or to exploit inherent opportunities.

To simplify matters somewhat, subsequent sections of this report are presented from the perspective of the Electronic

Information Exchange System (EIES) of the Center for Computerized Conferencing and Communications at the New Jersey Institute of Technology. EIES has been chosen for this exposition, not only because it is the computerized conferencing system most familiar to the author, but because it probably is the system most advanced in terms of developed applications and of use by a diverse audience of members.

Turoff and Hiltz (1977) have identified four fundamental services that have been incorporated in EIES.

Notebooks	Personal communication space that may be shared with co-authors, for the developing and editing of documents
Messaging	Dyadic or group communication space
Conferencing	Closed group communication space
Bulletins	Public communication space for on-line newsletters or journals

They identify ten additional services that are in various stages of development for computerized conferencing, four of which may be of some importance to the current discussion:

Form generation and collection,

A microprocessor that functions as a full-fledged conference member,

Model and simulation activities,

Directory.

All these applications can present both opportunities and pitfalls in uses entailing privacy, confidentiality or anonymity.

In this section the opportunities will be explored; in the following section the pitfalls that have been noted to date will be discussed. It must be emphasized that although EIES bears strong resemblance to the salient features of most other computerized conferencing systems, both major and minor hardware and software differences in other systems could impose different programmed conventions with consequent differences in adaptive social conventions.

Notebooks can be regarded as either private or confidential instruments. Privately, the individual can use the notebook to record, copy, arrange and synthesize thoughts and information in the manner that people in the past have used scrapbooks, diaries, filing cabinets and manuscript drafts. These private thoughts and syntheses can be shared with confidentiality.

- § A joint private space or notebook can be created by inviting co-authors to assist in composition, critique and editing.
- § Editors, peers, referees and others can be shown notebook contents with an understanding that they are not to be divulged to third parties without permission.
- § Copies may be made for confidential perusal by others.

The notebook owner is the only person who knows which other members have access to the notebook; that is, those entering items into it will know who else may be reading their comments only if the owner chooses to tell them.

Messaging presents the same opportunities, but programming conventions and early user behavior indicate that the recipients of messages can more readily transfer message contents to third parties electronically. The application of copyright laws to computerized conferencing communications is not always clear, but some have suggested that the recipient of a message can share in its ownership; that is, rights of confidentiality may be achieved only through observance of social protocol developed to protect those rights by mutual agreement by both the sender and the receiver of the item.

Conferencing precludes privacy, but members could agree to confidentiality, and programming can be used to conduct all or part of a conference through anonymous interchange by participants who can elect or be constrained to enter their remarks under labels of "anonymous" or by use of pen names. The anonymous label is the more secure device in terms of preserving anonymity, but the pen name facilitates interchange by allowing other participants to follow a particular chain of thought or to direct questions and remarks to a specific participant.

The Bulletin in its preparation provides opportunities for anonymous interchange among authors, referees and editors. In its promulgation it can be employed as a forum for the anonymous expression of dissenting views, particularly those that may be politically or socially unpopular. Through use of pen names it can then become a public place for anonymous debate of those views.

Form generation and collection can be viewed as the computerized conferencing equivalent or application of structured group processes such as survey research and delphi studies. As such, it can function in much the same manner as the mail survey technique described in Section II, but at greater speed, and with enhanced features such as programmed instruction to use filtering and branching devices in questionnaires automatically, to offer systematic explanatory notes, or to create possibilities for interviewer/respondent interaction that cannot be attained in mail correspondence. In this manner, computerized conferencing can be employed to administer the simplest data gathering instrument or highly complex interactive tasks that synthesize a variety of group process techniques. Operationally, respondents can be granted confidentiality or true anonymity according to constraints presented in the particular exercise [15].

A microprocessor can be used to facilitate confidential and anonymous data collection. It can serve as an electronic

"interviewer" that has no interest in the identity of an individual save for processing purposes, and such entries can be erased permanently once preset conditions have been satisfied, e.g., prevention of double-voting, unauthorized voting, etc. Its ability to transfer information, however, can create problems as will be discussed in Section IV.

Modeling and Simulation activities can be regarded as enhanced structural versions of messaging, conferencing and data collection. In addition, the activities could be employed to compensate for whatever a researcher may feel is lost in not possessing the identity of anonymous participants engaging in the activities.

A particularly interesting application is suggested by Scher's (1977) review of Zuckerman and Horn's analysis of simulation game communication processes (1973) in which he concluded that computerized conferencing "...is in an outstanding position through its ... capability for anonymity (capability for deceit)." Within the current context this observation can be noteworthy on two accounts;

1. It suggests that anonymity, used as a deceitful mechanism, may serve as a positive disruptive force in some future applications of computerized conferencing.
2. By inference it could suggest that unmasking anonymous communications, although undesirable in conventional communications and problem-

solving activities, could be desirable in some artificial game modes that may be introduced in computerized conferencing.

In the latter regard, it should be noted that communications intelligence in the form of intercept and identification most peculiarly is not a normal function in simulation conflicts, eventhough it can be a critically important component of real life conflicts [16].

The Directory contains the names of computerized conferencing network members, together with their mailing addresses, telephone numbers, and self-descriptions of characteristics and interests [17]. Associated programming permits other network members to obtain these descriptions or to conduct profile searches based upon key words to locate individuals with similar interests, or living in a given geographical area as defined by a postal zone or telephone area code. Although the directory promotes obvious advantages in presenting the means through which individuals of similar interests or propinquity can locate one another, it potentially is the source of abuses akin to those currently encountered through telephone directories and mailing lists: the computerized conferencing equivalents of crank or even obscene telephone calls may eventually be met, lists may be sold to commerical interests, and descriptions could be utilized by marketing researchers to isolate above-average prospects for goods and services.

The directory probably already serves to contradict an

important asset of computerized conferencing, cueing anonymity. As a verbal medium with only very limited graphic capability in present form, computerized conferencing constrains network members to judge received ideas largely in terms of their intrinsic, expressed merit, rather than by such potentially distracting elements as the ad hominem characteristics of the ideas' generators. This functional partial anonymity allows one to judge an idea without reference to tone of voice, oral emphasis, ambience of setting, facial expressions, body language, or similar non-verbal cues. In cases where conferees have not met face-to-face previously, judgments can be rendered without reference to physical appearance, age, perceived physical attractiveness [18], dress, or even sex [19]. A complete dossier can do much to reduce this advantage if it contains information that counteracts this aspect of anonymity [20].

Currently, directory information almost exclusively presents positive information about network members. Potentially, anonymous directory entries could be established that would allow members to establish connections for the exchange of information on socially-undesirable or sensitive issues or characteristics. Computerized conferencing could generate the electronic communications equivalent of the "anonymous" or telephonic "hot line" to enable members who wish to discuss such topics as alcoholism, gambling addiction, narcotics addiction, overweightedness,

homosexuality, extreme political opinions, and so forth, to contact others with similar problems, inclinations or expertise in the topics. Through use of pen names, such contacts could be truly anonymous in contrast to current encounters that frequently are only confidential, and compromised to the extent that disclosure or fear of disclosure is present.

Another major component of computerized conferencing, that at the time of this writing was in developmental stages, is the collection. The collection is a structuring device through which individual members or conferencing groups may define computerized conferencing items, and organize them according to personal or group preference. Although citational schema for authors are commonplace in other computerized systems, the EIES collection procedure goes further and allows the collector to list items authored by other members and even to incorporate listings of items from data files or documents not contained in EIES. The collection does not copy anything but merely references other existing items and allows whoever can read the collection to peruse those other items [21].

While collections are likely to be used initially by members and groups to organize notebooks and bibliographies, they also have the potential for becoming a structured means through which attribution and priority of contribution to group enterprises may be established and documented. In this

manner the group as it moves towards a consensus position would relegate each relevant contribution to the enterprise to its proper place. Retrospective searches of the final collection structure, and of interim structures, could be used to document the relative contribution of each member to the final outcome of the group's discussion or experimentation. In extreme cases in which a group member or sub-group of members disagreed with the consensus position of that process, as delineated by the overall group's collection, "minority collections" could be compiled to advance alternative interpretations of the group's progress and findings. The majority and minority versions could then be submitted to mutually acceptable peers for arbitration.

Part or all of the discussion and experimentation, as synthesized and documented through collections could be conducted through anonymous or pen name communication. At a later date, as in a poker game, the true identities of the authors of successful ideas could be revealed at each author's option. By the same token, however, unsuccessful ideas, that authors would just as soon have everyone forget about, could be consigned to anonymous oblivion. It is hypothesized that the combination of collections and anonymity should foster freer and more productive group processes. All members of a group would be assured that their ideas, even when given anonynously, utlimately would be

properly acknowledged. Unpopular or highly speculative concepts could be advanced without fear of ridicule, recrimination or loss of peer standing, and anonymous challenge to any idea communicated could be made with similar protection. This promises to be a major shift from the results of more conventional media which frequently are characterized by reluctance to advance unpopular or nascent concepts, or to criticize the contributions of other group members, especially those who are superiors or acknowledged experts in the field of inquiry. Hiltz (1977), for example, has hypothesized that,

> "...negative reactions (Bale's categories 10, 11 and 12) will represent considerably higher proportions of computerized conferencing comments, <u>especially if the capability for anonymous statements is present in the system</u>.... this should be an advantage of computer conferencing as a communication mode for problem-solving, since it would represent less reluctance to criticize bad ideas, and should lead to more frequent high quality solutions." [Emphasis added.]

The collection, however, can pose some threats to confidentiality. As it allows anyone viewing a collection of titles to obtain also the original texts, the conditions for inadvertent disclosure of confidential materials to third parties are enhanced.

<u>Pseudonyms and Masks</u>

The participant nature of computerized conferencing tends to produce procedures, conventions and protocols that are user-defined. This condtion has lead to new applications of the use of pen names beyond those originally envisioned.

Kerr (1977) probably was the first to point out and practice the use of the pen name in computerized conferencing as a social convention.

> "I use my pen name not in terms of cueing, but perhaps as what may be called protocol, something of a political sense to it, an agreement among friends to message each other in humorous ways. Sometimes in conferences, when I know it won't be anonymous, but when I want to make a point of this current self-definition.
>
> That is, I see a real distinction between my use of my pen name and those occasions when I choose to be anonymous; the first is humorous and friendly, the second tends to be biting and sarcastic. But even the second has never been used in serious conferences to stab someone."

Wellman (1978) carries this theme one step further and sees the use of pen names as masks that could enable their users to agree to suspend social conventions.

> "...rereading Durrell's <u>The Alexandria Quartet</u>, I was struck by the similarities between a masquerade and pen names in EIES. That is, it is not too tough to figure out who a pen name 'really' is, but even so they are useful. They are a way of distancing yourself from your own identity, and more importantly, your routine set of social roles, so that you can do/say new things. The masquerades (the classical Durrell kinds with black domino masks and balls in multiroom mansions) allowed people to say/do such things as carrying on affairs which they normally could not get into. Although most people 'knew' who each other were, the distancing effect of the mask allowed the polite fiction of anonymous liberty."

In this same context a group of EIES members in an informal conference once adopted such identities as "Francois Marie Arouet," "Madame Du Chatelet," and "Diderot," and conducted their exchange in French in the manner of a salon dialogue of the period.

The potential for future development of complex masks and contrived social settings through computerized conferencing may be great. One can speculate that individuals will establish separate directory listings to match the traits portrayed by their masking pen names. Such descriptions could be particularly beneficial for those afflicted with psychological disorders entailing multiple personalities as a means of delineating their separate characters for themselves and those who seek to help them. In more rational discourse devil's advocacy could be raised to a refined level through adoption or assignment of stereotyped stances reflecting desirable points of view. Members of a conference itself, in addition to adopting or being assigned roles, could be constrained to conduct their dialogue in a manner reflecting an historical model, e.g., a socratic dialogue, a French salon, a discussion among the Encyclopaedists, an English science club, etc.

SECTION IV: Barriers

Experimentation and use of computerized conferencing to date has been confined largely to comparatively elite groups of scientists, technologists and advanced students, many of whom have received their primary training in the physical or information sciences, and may thereby not be fully aware of the ethical considerations surrounding rights of network members to privacy, confidentiality or anonymity. Fortunately, most if not all, bring to the enterprise codes of ethics and practices developed through academic or professional practice that mitigate very strongly against any exploitation of their fellow members. It could be surmised, however, that as computerized conferencing is extended to a more general population, that members will then include the usual assortment of knaves and fools. It would seem imperative to design safeguards that would forestall the former and protect the latter.

Some early computerized conferencing developers and experimenters have engaged in "fun and games" activities that have arisen spontaneously in recognition that anonymous functions promised for the medium can be compromised under extant programming and systems design. Pen names, for example, can be compromised through the following observed phenomena.

Time Coincidence

Synchronously-received anonymous items can be cross-referenced to members currently on line in the network at the time of receipt. Asynchronously-received items can be checked against suspected senders' last period of activity as listed in their directory descriptions.

Traffic Analysis

Participants tend to conform to set patterns of usage according to time of day, days of the week, and frequency of use. Examples: early sign-on, checking for messages before the end of the business day, types of items composed and transmitted during evening hours, use during weekends. Geographic location frequently can be noted because of time zones, e.g., eastcoast participants sign on early; westcoast participants are more likely to sign on later in the day.

Participation

Participants have a choice of a number of private and public conferences. Listing of those participating in the private conferences is available, as is a marker system denoting each member's progress in perusing the items in the conference. Listings and markers of this type are not available in public conferences, but participation gradually can be determined through noting contributors' names and through references to the conferences in other contexts.

Response Time

Members often vary according to their usual speed of response. Some answer questions or enter comments in

synchronous sequence or at least within an hour. Others respond over a lengthier period of time.

Editing Sophistication

A wide range of sophisticated word processing and programming techniques is available in advanced computerized conferencing systems. Naturally, relative sophistication in utilizing these devices to set formats, make corrections, display ideas graphically, etc. varies widely, as does the time lag between introduction of a new feature and its adoption for use by individual members. Newer members in a conferencing group may be conspicuous simply through observation of common new-user mistakes.

Writing Characteristics

Individual traits are displayed and recognized in terms of consistent spelling errors, typographical errors, use of abbreviations, common expressions, and use of jargon.

Terminal Characteristics

Some terminals can be used to send messages in both upper and lower case characters, others in upper or lower but not both, and others in upper case only (TTY). Those members having an option between upper and lower case generally appear to tend towards use of lower case for identified communications, but, interestingly, frequently appear to switch to upper case when communicating in an anonymous mode. Some terminals may be limited in terms of special characters, so that presence or abscence of symbols

can be discerned.

Subjective Style

Probably the most difficult characteristic of all to mask is one's writing style which can serve as a personal "fingerprint" for each communication. It seems likely that Fogg and Flesch readability-type measurements could be developed to identify individual authors. Intuitively, members in constant contact over a period of time come to recognize each other's individual styles through observation of such things as paragraph and sentence length, word sequence, vocabulary, grammatical form preference, and punctuation.

Boasting

Some participants cannot seem to resist the temptation to twit others about the source of anonymous remarks; others will confess to being the authors of anonymous traffic; some will attempt to mask the anonymous items through public comments that express wonderment about their source; and others simply will "protest too much."

Compromise

Inadvertently, an anonymous item might be entered that through time coincidence or subject reference immediately establishes a sole or limited range of sources. Triangular coincidence can occur when party "C" refers to a matter ennunciated by party "B" that identifies an item received earlier by party "A". Mechanical errors are very rare, but

when they do occur, inadvertent disclosure or compromise of private, confidential or anonymous traffic can take place. Somewhat more frequently, compromise can occur in the process of introducing new programming features that may offer opportunities for unforeseen disclosure before they have been thoroughly tested and debugged.

Decoder Silence

One of the subtlest rules of decoding anonymous identities is not to reveal success, but to maintain silence so that the compromised party does not alter pen names or traffic patterns, and so that others will not be alerted to potential dangers. A patient traffic analyst in this manner can reconstruct an entire network's anonymous identities over an extended period of time.

Few of the techniques discussed above in and by themselves will reveal the identity of a member making anonymous remarks, but used in combination, even one who is deliberately trying not to guess at identities is apt to see through the masking intuitively. Because of frequent lack of sophistication in such matters by many, even the careful practitioner of anonymity stands ultimately to be revealed through a simple process of elimination.

When it is considered that in times of war and in diplomatic intrigue, encrypted communications conveyed by highly sophisticated electronic means ultimately have been decoded and identified with spectacularly successful (or disastrous)

consequences, computerized conferencing traffic analysis would appear to be child's play by comparison.

Security

As in any computerized system, computerized conferencing's provisions for privacy, confidentiality and anonymity ultimately can be compromised through sureptitious entry into the host computer's data files. The degree of privacy afforded by a computerized conferencing system to the individual for use in private or confidential spaces will be dependent upon the security effectiveness of the system itself and the integrity of its implementors and operators. By definition, private and confidential spaces, and identification of adopted anonymous masks, are not matters to be shared with others and entry to such contents can be gained by another only through illegal means. Unfortunately, even the most secure system can be compromised by a determined, knowledgable person who can either pose as a legitimate user, or worse, gain entry to the system's programming structure, move freely within all system files, and then erase any evidence of illegal entry.

It probably can be safely assumed that few, if any, conference members would attempt to secure illegal advantages for themselves. Further, the mature computer conferencer is not likely to pursue any elaborate course of traffic analysis, because of recognition that privacy, confidentiality and anonymity functions can be of mutual

benefit to all members. This assumption notwithstanding, however, current system design inadequacies and participant naivete can combine to aid inadvertent disclosures of anonymous identities.

Confidentiality Protocol

Confidentiality poses problems that cannot always be aided simply through enhanced design or programmed safeguards, because it relies more upon the mutual trust of all members concerned. The fragility of this trust was well demonstrated in one heated debate that took place in an informal conference. (See Appendix C for a transcript of the debate.) A member of the conference took strong issue with the current suggested protocol for treatment of confidential items.

> "If a private message is sent to you, it is considered a a breach of confidence to copy it to another person without explicit permission from the author. Because it is very easy to copy to others the messages one receives, without this norm of asking permission to copy, one could never be sure that confidential messages would remain so.
>
> If you send a message to someone like a conference moderator and you don't mind if it is copied into the conference or to other conference members, say so explicitly [22]."

The individual who objected to this protocol rested his arguments against its adoption on assumptions that it:

- § is uneforcable,
- § does not rest on any current legal rights,
- § could contradict other conventions that the source of ideas should always be acknowledged,

§ inhibits free speech,

§ would be an incumberance entailing separate agreement with all correspondents.

Unfortunately, the only substitute agreements he offered are reducible to "let the sender beware" or "trust me" conventions.

Neither of these suggested substitute protocols were at all agreeable to the other conferees in the debate, who instead suggested that failure to adhere to confidentiality conventions and courtesies could:

§ compromise and take advantage of the naivete and trust of the new conferee,

§ lead to uncertainty and inhibit personal communications,

§ entrap anyone not aware of a receiver's presumed "right" to compromise any assumed confidentiality,

§ inhibit side discussions considered necessary for clarification or for preparation of more formal public remarks,

§ lead to conditions of alienation in extreme cases.

Those endorsing the EIES confidentiality protocol argued that it could be enhanced by:

§ requirement of explicit statements of intent by anyone not intending to abide by it,

§ insertion of explicit instruction to not copy any communications considered to be especially confidential,

§ use of discretion in communicating confidential matters until such time a new correspondent is known well enough to be entrusted in such matters,

- § addition of programmed conventions that would disallow at the sender's option, a message to be copied,

- § or, all else failing, discipline of the asocial behavior in this regard through extreme reduction or total suppression of all further communication with the miscreant party.

A false sense of confidentiality can be created through the use of blind copies of messages. Normally, the addresses of messages are indicated in the message banner, but some systems allow the sender to suppress this information. This could create the false illusion for the receiver that he or she is the sole recipient of the message, when in fact others may be receiving it as well. In formal experimental settings blind copies might very well be sent to experiment monitors without the knowledge of the experimental subjects to whom they ostensibly are directed exclusively. This practice could call into question concerns about human subject rights. Blind copying of the subjects' own messages to a monitor without their knowledge would, of course, be a case of simple electronic eavesdropping.

Anonymity Abuses

Additional abuses of anonymity functions have been hypothesized and tested through the fun and games of early computerized conferencing experimenters. First, pen names can be misappropriated by others if programming constraints against this practice are not present. Very simply: one could use a recognized pen name as one's own and create

mischief. One could even set a proper name of a member as a pen name if safeguards are not taken. Such manipulation could be very subtle and deceiving to the uninitiated who are unaware of computer programming capabilities. For example, programs could be set that would allow only one person to enter a given name or pen name, but a clever computer forger could make use of non-visual characters to fool some programs, e.g., set John (space) Smith as John (control key) Smith. In the example given, both forms would appear identical on the printed transcript or CRT screen display, but would be treated as being quite distinct by the system's central processing unit.

Secondly, it is assumed that as computerized conferencing becomes more widespread, it will become prone to such annoyances of alternative communications media as abusive or obscene messages sent by anonymous or pen name mode. The problem would be compounded by the misuse of the pen name as suggested above; that is, asocial messages sent under a misappropriated name or pen name would create even greater mischief.

Interfacing Compromises

In the future as computerized conferencing systems proliferate and as larger networks are formed and microprocessors and other hardware are used to interface a given system with other systems, both programmed and

social conventions may be altered in ways that would pose threats to members' rights to privacy, confidentiality and anonymity. The means for electronic transfer to another system would exist and that system might not contain the same programmed safeguards found in the system in which the member originally enters an item. Once an item is transferred to another system the author may no longer have a say in the social conventions governing protocols concerned with the protection of privacy, confidentiality and anonymity. Further, for very valid reasons, a person who participates in more than one computerized conferencing system, may just as soon not have system "A" know that equivalent or related data are being used in system "B" [23].

Monitoring Abuses

Computer systems are susceptible to monitoring by outside agencies. Hiltz and Turoff (1978) suggest that systems could be programmed to check traffic for certain words and phrases and inform authorities when a word such as "murder" has occurred so they could then obtain a warrant to read the item. They report that some suggest this could be considered the right of police to patrol but not a violation of privacy or eavesdropping because no human has actually read or "heard" the item text. Although this reasoning may sound quite sophistic, stranger events have occurred in the name of "law and order" or "national defense."

SECTION V: Suggested Enhancements

Security

Ultimately, the most effective means to protect privacy and to maintain confidentiality and anonymity in telecommunications probably will be attained through the use of computer-assisted cipher encoding and decoding. Until relatively recently the only truly unbreakable cipher has been the "one-time pad;" a random number-based system that is successful, but both time-consuming and logistically complex in its administration. A more promising method has been suggested by Gardner (1977), and is based upon the "trapdoor codes" of Diffie and Hellman (1975) and the subsequent proposal for the use of prime number signatures for such codes by Rivest et al. (1977). Operationally, codes of this type promise the development of double encoding mechanisms utilizing encoding and decoding algorithms which feature unique identifiers for both sender and receiver based upon factors of prime numbers. The ciphering system is such that the encoding mechanism can be made public, so that it would have practical use in group situations as in computerized conferencing, but the decoding algorithm for each member is maintained in secrecy. Without the decoding algorithm, it has been estimated that current computer technology

would require millions of years to decipher the encoded text. The procedure also provides a unique signature for each member so that no member's signature can be forged. It would appear to be just a matter of time before appropriate hardware and software will be developed for the automatic, user-transparent implementation of these methods for public use in applications such as computerized conferencing.

Member Rights

The form feature could be used to inform computerized conferencing members of their rights to confidentiality and anonymity. Statements devised by a conferencing group or those embodying the requirements of federal regulations or professional codes of ethics regarding the rights of experimental subjects could be transmitted to the members as a message form. The participants' receipt of the form would be registered automatically and the sender would receive written confirmation of the date and time of receipt. More positive acknowledgment could be obtained by also including within the form a question form such as that shown below.

> I HAVE READ, UNDERSTOOD AND AGREE TO THE CONDITIONS GOVERNING MY PARTICIPATION IN THE EXERCISE. (Y/N/?)
>
> [if ?]
>
> I REQUIRE THE FOLLOWING INFORMATION BEFORE AGREEING TO PARTICIPATE: (ENTER YOUR QUESTIONS HERE.)

The use of such a form would provide several distinct advantages over current methods: 1) It provides both the

member and the experimenter or group leader with full documentation of all agreements. 2) Participant questions can be answered directly by the experimenter or group leader instead of through an intermediary such as a survey interviewer or computer console operator who may not be as qualified to understand all aspects and implications of the questions. 3) The asynchronous nature of computerized conferencing gives the participant sufficient time to consider the question of participation before reaching a decision. 4) Interaction should be less awkward than what may occur when an interviewer or other agent reads to the participant his/her rights in the fashion of a police officer reading to a criminal his/her rights to remain silent.

Special protocols may have to be developed to protect member rights of confidentiality in notebooks. Because a notebook owner is the only person with direct knowledge of who else is reading the notebook, the potential for entrapment of confidential material by third parties unknown to an author will exist. This problem could be alleviated through requirements that a notebook owner either inform all notebook authors of who else has access to the notebook, or that a statement be given to all potential authors that anonymous readers of the notebook are present.

Thwarting Inadvertent Disclosure

System programming could be employed to eliminate some sources of anonymous unmasking.

- § Anonymous or pen name items could be converted automatically to TTY (upper case only) format.
- § Special terminal characters, especially control key functions, not commonly encountered could be disallowed in pen name communication.
- § User-specified or systematic time delays could be incorporated to eliminate establishment of time coincidence disclosure. (Such a feature would have to vary according to context; a synchronous activity might feature a maximum delay of ten minutes' duration, an asynchronous conference might allow a maximum of 48 hours.)
- § Future developments in word processing would eliminate common misspellings. As EIES Interact language evolves, users may very well develop their own procedures to edit for the elimination of such self-recognized problems as poor spelling, split infinitives, dangled participles, and sentences ended with prepositions.

Preventing Misappropriation of Pen Name

When members are given a free hand in setting or changing pen names, potential abuse, as discussed earlier, exists for using a pen name to mimic the proper name or pen name of another member. This potential abuse has been forestalled by two principal means: 1) at the elementary level of programmed conventions that do not allow the use of another member's name as a pen name; 2) by the use of distinctive identifying marks such as "John Smith" or *John Smith* to denote that the name is a pen name.

The mimicry of pen names or their cognates could be forestalled through adoption of programmed conventions that would disallow further use of any pen name previously, but not necessarily still being used, entered for a given period of time, e.g., the duration of an exercise, 30 days, six months, one year.

Confusion can occur when pen names are used to mimic official-sounding titles such as system monitoring titles, government agency designations, or institutions. Social conventions disallowing the use of such names could be established and reinforced by authorization of system monitors to censor out any such pen names as they occur.

Minimizing Misapplication of Pen Names

The social use of pen names discussed earlier, although useful in some contexts, can become a liability in more serious discussions. The user of the pen name could adopt uncharacteristic attributes associated with the self-perception of the pen name, and other conference members could attribute positive or negative characteristics to its user. To cite just two examples observed in EIES conferences: "Wonder Woman" for some might evoke images of a militant feminist, and "Alvey Singer" of a Woody Allen-type eccentric. This creates a synthetic problem in which the original purpose of the pen name, the creation of anonymity and elimination of ad hominem judgments, is replaced by

potentially complex fictitious assumptions about an idea's generator.

The resolution of this problem would appear to lie in the use of the military-type code book compilation of blocks of standard pen names that could be allocated to groups for use by their members. Each member would be assigned one or more names to be used within the group. (Cross-group usage would simply aid others in establishing identification through elimination processes.) The names would have to be selected carefully to minimize hierarchical, ordinal or anthropomorphizing effects. For example, proper nouns of natural objects could be used, such as:

> Ash, Beech, Birch, Maple, Teak (but not Oak or Ebony)
>
> Mallard, Oriole, Sparrow, Tanager, Wren (but not Hawk, Dove or Loon!)

Member Item Deletion Control

One of the simplest, but most effective means for providing privacy and confidentiality is to allow a member to delete an item. Quite commonly, members in most systems may delete any item they originally authored. In a private space such as a notebook this presents few problems. In a confidential space such as a message system or conference problems can occur because those receiving an item may be able to copy it before the author has a chance to delete it.

This difficulty could be overcome by programming conventions that would allow an author to specify that an item be deleted automatically upon receipt.

There are occasions when the receiver of a message may wish to be able to exercise the privilege of deleting it because it is felt it contains information that should not be a matter of record or copied elsewhere. Programmed conventions could be developed to provide this option.

Members should be fully informed of the computerized conferencing system's definition of "deletion." To some it might come as a surprise to learn that an item that to their mind has been deleted may still actually exist in the computer memory, because only the system link to that item has been deleted. In such cases the potential exists for an operator to retrieve the supposedly deleted item. In those systems in which the memory supposedly has been erased as a condition of deletion, the potential for recovering the erased item may still exist. Expensive devices have been developed to recover computer memory information that has been accidentally erased, and such devices since they deal with digitalized data can be more effective than those used in attempts to recover the complex impulses of erased audio recording tapes.

Member Reception Control

As currently constituted, computerized conferencing

gives the individual member little control over messages that are sent to the member. Currently this presents difficulties only in terms of information overload, viz., lengthy items from verbose correspondents that arrive at inopportune times. This generally creates only minor and transient problems. The potential, however, for receiving truly unwanted material, ranging from junk mail to obscene or threatening messages sent anonymously, creates a need for greater user control of reception. Fortunately, computer architecture creates possibilities for exercising such control without involving system operators in complex questions of carrier responsibilities and ethics; that is, systems can be programmed to exclude classes of items upon reasonable user request without any human operator having to have knowledge of the excluded senders, or for that matter, of those requesting such exclusions.

§ In the case of nuisance items such as those that may contain obscene material and which are sent anonymously, programs could be devised by which a user upon receiving such an item could enter a command that would tell the system that no further items that are unsigned (anonymous or pen name) can be transmitted to the user from the member who sent the miscreant item. The anonymous messager in such an instance would be informed of this condition

upon trying to send any further anonymous items addressed to the aggrieved party.

§ Program conventions could be introduced to prevent the transmission of such matters as obscene words or racist pejorative words. (Such conventions, however, would have to be examined carefully to determine the extent to which they could constitute prior censorship.)

§ To cut down the flow of computerized conferencing junk mail equivalents, conventions could be established that: 1) Members can request their names be removed from any address lists for prespecified classes or origins of traffic; that is, obtain rights to removal from lists as can be obtained in conventional mailing operations. 2) In recognition that some unsolicited items can be of potential, but unpredictable, value, senders of such materials could be assessed full costs of sending and receiving.

Confirmation

Ultimately, the seemingly innocuous confirmation of received items could become an important aspect of computerized conferencing communications. Unlike most conventional telecommunications media, the sender of an item

does not always have assurance that the person receiving an item is the intended person: it could very well be received by an operator using the terminal on the designated recipient's behalf or by someone who is sharing the intended recipient's network membership. The sender may not always be aware of such conditions and could be trapped into sending information not intended for third parties. Currently, the only practical resolution of this problem is to restrict sending of such items to times when prior synchronous assurance has been obtained from the intended recipient that he/she is in fact utilizing the receiving terminal and that others are not present. In the future, personal decoding algorithms, as discussed earlier, should circumvent this problem. (Their use would also constitute certification of receipt.)

Interfacing Conventions

The problems that will be created through the interfacing of computerized conferencing networks or through conference access and transmittal to other computerized systems are far from clear, but it is anticipated that conferencers will find themselves confronting problems not unlike those now created through merger of data files by government and private agencies.

As microprocessor and other computer-assisted interfacing capabilities emerge it may become necessary to develop

concomitant programmed conventions to ensure that conferencers' rights are not compromised inadvertently or through malevolent action by those understanding the weaknesses of such arrangements. At this time three constraints that could be imposed on an interfacing system can be hypothesized.

1. Members should receive automatic notification upon each and every instance that information they have authored in a conferencing system or information about their behavior in using that system is transferred outside the system.

2. Protocols and conventions should be developed through which categories of member information or member-authored items can be transferred only with prior and explicit consent by the member.

3. Members should never be required to rely solely upon system facilities to undertake all transfer operations, but should be given options to undertake these activities themselves through whatever off-line channels they may have access to. In this manner, the individual member can exercise greater control over private, confidential or anonymous intellectual and behavioral property.

Expediency vs. Participation

Undoubtedly, implementation of these suggestions and other safeguards undertaken to protect computerized

conferencing members' rights to privacy, confidentiality and anonymity will prove to be irksome in some instances to members, conference operators and conference leaders alike. It must always be borne in mind, however, that what may sometimes appear initially to be a programming barrier or impediment to smooth communications or group processes, may in fact later prove to be an important element that will actually improve upon those processes. In the final analysis, human rights and intellectual and psychological freedom can be at stake in these issues, and "expediency" and the natural desire to attain quick implementation of exciting new technologies should never be allowed to compromise the human element that constitutes the very reason for their development.

The early experience of computerized conferencing has suggested that it has outstanding potential to become a truly participant-directed computerized medium. Unlike most other computer applications, computerized conferencing leads to hands-on experience for its members. Most, after they overcome the short initial mechanical difficulties, become quite adept at using the new system. To their pleasant surprise they discover that they do not require support personnel to assist them in the use of their terminals and that they can perform a wide range of functions for themselves. Once this confidence has been acquired, many then turn to the system itself and to varying degrees ask, or even demand, to

participate in its further design and refinement. By the same token, system operators and designers are confronted with sophisticated users who no longer passively acquiesce to their decisions, but to their surprise offer counter-suggestions for system enhancement. At this point the line between users and implementors becomes increasingly blurred. Implementors find they must accomodate user-defined social conventions, and special languages such as EIES Interact are evolving to permit users to construct their own programmed conventions and structures within the system.

This trend undoubtedly will continue, and computerized conferencing systems will become more participant-defined in their applications. In the context of the current discussion, this should mean that network members will be in a better position to ensure the protection of their rights to privacy, confidentiality and anonymity.

It is likely that some groups, notably those that are industrial, military or governmental in orientation, will at least initially resist participant direction. They may be expected to desire the retention of more conventional organization hierarchies and knowledge of the communications by subordinate members. It should be interesting to note the ways, if any, in which such stances in turn will succumb to member demands for greater participation in conferencing processes and structural definition. Future experience may

demonstrate that organizations may evolve in ways that will replace centralized and hierachical structures with decentralized participant structures.

SECTION VI: Conclusions

Historically, privacy, confidentiality and anonymity have facilitated cognitive interaction. The development of computerized conferencing both enhances and presents new challenges to these conditions.

Computerized conferencing for the first time offers facile and effective anonymous communication within a structured environment. As such, it facilitates the attainment of a long-sought goal: the judgment of ideas and information without respect to their origins or distracting *ad hominem* cueing elements. This development both improves upon previous communications modes and creates opportunities for the construction of more sophisticated group interaction mechanisms attuned to the complex needs of contemporary science and society.

As is the case with most technological developments, computerized conferencing has been handicapped initially by psychological and mechanical shortcomings encountered in the transition from the previous technology to the new technology and its associated cognitive structures. It would appear, however, that as experience is gained through use of the new medium, structured means are being developed to overcome the barriers that compromise the effective use of privacy, confidentiality and anonymity.

Cognitively, computerized conferencing creates an environment in which the proper relation of private to public ideas is better understood. Mechanically, programming structures are being developed to protect user privacy and to employ confidential and anonymous modes properly in promulgation of group members' private cognitive property into syntheses of policy and scientific structures.

It is hypothesized that through computerized conferencing, privacy, confidentiality and anonymity will develop into formal, recognized modes of expression and cognition that will be beneficial to both individuals and to the society of which they are a part.

APPENDIX A: Nomenclature

In contemporary usage, "privacy," "confidentiality" and "anonymity" unfortunately frequently are treated by many as synonyms. Roget's Thesaurus, for example, lists privacy and confidentiality as synonyms, and further appears to emphasize their association to the pejorative aspects of the terms, e.g., stealthy, sly, underhanded. Confusion of these terms with anonymity is rarer, but in the survey research field at least, confusion of anonymity with confidentiality appears to be relatively commonplace.

Dictionary definitions appear to assign more specific meanings to the terms. Consider first, the meanings of privacy that seem pertinent to this inquiry.*

> Privacy 1. The state or condition of being withdrawn from the society of others, or from public interest; seclusion.
>
> 2. Private or retired places; private apartments; places of retreat.
>
> b. A secret place, a place of concealment.
>
> 3. Abscence or avoidance of publicity or display; a condition approaching to secrecy or concealment.
>
> 4. A private matter, a secret.
>
> 5. Intimacy, confidential relations.
>
> 6. The state of being privy to some act.

*The definitiions cited in this Appendix are taken from the Oxford English Dictionary (OED). Only those definitions pertinent to the scope of this report have been included.

Private 1. Withdrawn or separated from the public body.

3. Kept or removed from public view or knowledge; not within the cognizance of people generally; concealed, secret.

4. Of a thing: Not open to the public; restricted or intended for the use or enjoyment of particular and privileged persons.

c. In many connexions private is used to distinguish something that is not open to the public, or not publicly done or performed.

Although there is some suggestion in these definitions that there are confidential aspects of privacy, these definitions are listed secondarily to stronger senses of personal privacy. The sharing of privacy would seem to be done only in the most intimate or highly privileged manner. In this sense, current EIES nomenclature of "private notebooks" appears to be an appropriate use of privacy, but "private messages" would appear to be too broad a designation.

This interpretation appears to be reinforced by definitions of confidentiality.

Confidential 2. Of the nature of confidence; spoken or written in confidence; characterized by the communication of secrets or private matters. Confidential communication: a communication made between parties who stand in a confidential relation to each other, and therefore privileged in law.

3. Betokening private intimacy, or the confiding of private secrets.

4. Enjoying the confidence of another person; entrusted with secrets; charged with secret service.

Confidence 1. The mental attitude of trusting in or relying on a person or thing; firm trust, reliance, faith.

5. An object or ground of trust.

6. The confiding of private or secret matters to another; the relation of intimacy or trust between persons so confiding; confidential intimacy.

7. A confidential communication.

8. Trustworthiness, as a personal quality.

Confident 1. Trustful, confiding.

Confide 1. To trust or have faith; to put or place trust, repose confidence in.

4. To impart as a secret, to communicate in confidence.

5. To entrust (an object of care, a task, etc.) to a person, with reliance on his fidelity or competence.

Note above in particular that confidentiality entails elements of implied communication, trusting and trustworthiness not associated with privacy. The last definition cited is particularly interesting as it would appear to place the onus upon the receiver not only for fidelity, but for competence in maintaining that fidelity as well. The definitions associated with confidentiality would appear to be superior as a description for the implied trust in computerized conferencing messaging. At some future date, consideration might be given to labelling messages as "confidential messages" on the premise that recipients may be less prone to betray a confidence than to claim ownership of something which by definition, or only through extensive negotiation, may no longer be private. In certain instances, it might also be helpful to use terms such as "confidential notebooks" and "confidential conferences."

The definitions of anonymity are straight-forward, and suggest there should be little confusion with either privacy or confidentiality.

> Anonymous 1. Nameless, having no name; of unknown name.
>
> b. Hence ... A person whose name is not given, or is not known.
>
> 2. Bearing no author's name; of unknown or unavowed authorship.

The OED defines "pen name" simply as a pseudonym, but it is noteworthy that in the definition of anonymous, the suggested derivation is from the Greek ἀν (private) + ὄνυμα (name). In this sense it is the equivalent of the modern pen name.

PRIVACY AND OWNERSHIP

The written material in a system of this sort has a certain degree of uncertainty with respect to ownership under copyright regulation, common law treatment of mail or various laws governing computer data bases. However, our NSF contract contains the following:

> "Provide complete security and confidentiality of user's research information in transit through EIE(S) or stored in EIE(S).The Contractor will take all steps necessary to assure that data stored in the EIE(S) system will be confidential and that no one but the original user who stored the information and data will have access to these data. These data are the result of research projects not funded by this award."

Under this clause we shall do everything reasonable within budget and available technology to insure your privacy on an individual or group basis. We further interpret this clause to mean that we can refuse any requests from outside parties such as other government agencies for any EIES material. We shall, therefore, refuse to provide such information and will instead direct such parties to the author of the material requested.

However, I must point out that EIES is a Communication system as well as an Information system. We cannot take any responsibility for what use members of EIES make of any material directed to them by others. Thus, the system participants should be governed by the same ethical considerations governing

private or professional communications. We take the position that material entered in PUBLIC conferences, notebooks and bulletins may be quoted as one would with any other open publication. Therefore, authors should indicate in these public files when they are entering preliminary drafts whether it should or shouldn't be quoted (as one would normally do with a pre-print draft). As to private and group messages, private conferences and private notebooks, the individuals and groups involved must establish their own standards for handling the privacy of their material. Also, we hope the evaluators for each group will establish clear policies for his or her group.

You should be aware that the EIES technical staff can, if necessary, gain access to any material entered in the system. However, they are well aware of and sensitive to the need not to violate privacy. In some rare cases you may find a need to request us to fix something for you requiring that we exercise this power. In any such case you will be notified of this occurrence. For example, in a hardware malfunction, a data record of some sort may be damaged and the process of fixing it may require a check to verify that the right text item has been restored. Hopefully this will occur infrequently.

STATISTICAL DATA REPORTING

Our contract states in reference to our monthly progress report:

> "For each user and for each group of users the data will be presented under the following headings: number of messages or transactions, type of transaction (message, conference, etc.) and EIE(S) connect time."

Therefore, each month a statistical report will be furnished NSF listing each user's monthly and accumulated statistics for the following items in terms of sent/composed and received:

-- number of private messages
-- number of group messages
-- number of conference comments
-- number of notebook pages
-- hours of use
-- number of times on.

However, NSF has assured us that all they need is the information reported for an individual identified by a code which does not inform them of who the individual is. The key to the code will be kept at NJIT and the subset for any particular group will be provided the principle investigator for a particular group.

A copy of the NSF report will be provided each individual responsible for the evaluation of a particular group. In any internal evaluations of the EIES operation that we make ourselves it will be our policy in any of the resulting reports or papers to maintain the anonymity of users concerning the

representation or analyses of data on usage. We will request that all the group evaluators follow the same policy before we issue these reports to him or her.

For any particular group more detailed data will be available to the group's evaluator through the principle investigator and he or she will have policies for handling data derived from your group's activity.

However, I must point out that even without specific names mentioned, data presentations may make it easy for some participants on the system to identify certain members. For example, during the past year I have been the most frequent user and anyone else who has been using the system can identify my data point on any distribution of usage.

Together with the evaluators we hope in the next year to develop firmer concepts of what are meaningful measures of performance and impact in systems of this sort. We shall do our best to keep you informed of progress in this area.

APPENDIX C: Discussion of Copying of Prviate Messages

The moderator of an informal conference disagreed with the EIES protocol convention on message confidentiality, prompting the following heated and insightful exchange of opinion. (The names of the participants have been replaced by designations of PERSON A, PERSON B, etc.; pen names by "ALPHA," "BETA.")

C117 CC210 PERSON A 8/ 8/77 2:01 PM

I have just received the new instruction booklet for EIES [Turoff and Johnson-Lenz 1977] and would like to take exception to "3. Maintaining the Privacy of Private Messages."

1) It is impossible to enforce the not sending of messages onto others, and

2) I believe legal tradition gives letters to the person who receives them, and

3) I neither like to keep secrets nor wish to appropriate others' ideas as my own.

C117 CC211 PERSON B 8/ 8/77 9:19 PM

Re Person A's 210:

Knowing this is your point of view about privacy, I am going to be very careful about what I send to you as a private message. Several times already you have copied into conferences messages I have sent to you privately and never expected to see in a conference. So far, nothing embarrassing or too private has been shared, but I never know. As of now, I will only be sending messages to you, Person A, that I consider public. That may restrict my communication with you, but so be it.

C117 CC216 PERSON C 8/ 8/77 10:09 PM

Is this system like a letter or is it like the publication of an idea which you should be able to copyright or its equivalent. It's neither and a little of both. Afraid Person A, I agree with Person B.

C117 CC217 PERSON A 8/ 9/77 10:02 AM

I'm not sure how to put this. I would rather that Person B didn't send me something than that I had to consider it private. I agree with Person C that exactly what a msg is is a little difficult to define, but I would rather copy a msg than the ideas in it. Also, I would never want to make a profit at the expense of someone else's ideas.

Sometimes I do have the good sense to "not bother bringing something up." At least one person in this conference should realize that. If it is clear to me that something is sent privately, and it does not appear to be concerned with a shady or illegal matter, I won't bring it up with anyone else; but if someone is going to send me anything like that they should make that clear in the body of the text, and know that I am not happy to be receiving such messages. I feel this way for essentially the same reasons I got involved in a rather heated argument earlier.

This may be a bit brash, especially considering where I work; but as I indicated earlier, I don't intend to play by those rules. End of sermon...

C117 CC219 PERSON D 8/ 9/77 1:24 PM

I have to agree with Person B regarding the practice that has to be adopted in messaging you, Person A, and I feel I must follow the same policy.

Actually we or at least I should thank you for being so explicit about what you intend to do or not do, and therefore clarifying for us what to do when messaging you. But the rather petulant and obtuse attitude you continue to display in CC217 shows, I think, that you are missing the point about degrees of exclusivity or privacy which many of us find a valuable dimension of this system -- as it is in "regular" life -- and because you take the view you do you are cutting yourself off from a kind of relating and communication that this system offers.

It is not that shady or illegal matters are private, and everything else can be public. I hope we aren't discussing shady or illegal matters in "private" or here (this is just as public and just as private as telephones or telegrams, in general).

The point as I see it is that some things, perhaps often of a critical nature but sometimes also of a comforting or caring or connecting nature, come across much more authentically and fully if they can be said to the person

for whom they are intended alone. Not that I or we particularly want to have that kind of private access right now to you, but we might want to have it in the future, and we regret that that possibility is removed by your announced policy.

In general, if one wants to send a message to another on the system and wants to be sure that only that person does see it and does not copy it to others, this can simply be said at the beginning or end of the message. The recipient is then honor bound to abide by that request, or at least to request permission to copy saying to whom he/she wants to copy, to the original sender. Conceivably it should be possible to program the system to electronically "fix" some messages so that they could not be copied, and this would be a command added by the sender at the time of sending. But I hope that will not be done. It is better for our relationships to and with each other on this system if we manage our messaging with mutual respect for each other's wishes regarding confidentiality.

C117 CC223 PERSON B 8/ 9/77 2:25 PM

I sent a poem to my love
and hoped she'd hold it to her heart.

I didn't ask her to be discreet
Since I had written it just to her.

Why did she show it to her friends
who laughed, not knowing
that my heart sang
as I wrote?

C117 CC225 PERSON A 8/ 9/77 2:45 PM

My being is not me,
for I cannot see me,
but if you ask me to show myself
I'll show you you as me.

I talk in vicious cycles,
never knowing quite why
other's try to hide themselves,
and I can't show what I try.

Sing of joy, I cry...
but only tears prevail,
for what I see is
horrible
   I'll fight it 'till I die.

If I hide in platitudes, or
wallow in the mud...
I'm just as damned in solitude
as in the public flood.

No need to follow my path
You can as soon sink within your own.
But if you don't give me my path,
I'll damn your very bones.

(I'm going to add a warning to my description...)

C117 CC226 PERSON E 8/ 9/77 2:49 PM

About the privacy and copying issues: To me, it's simply a matter of trust, as Person B put so well earlier in this conference. Person A's CC210 was interpreted, by me and I think by others, as stating publicly that he can't be trusted. This copying norm has received some scattered attention on line; it is an important issue, but clearly also one that avoids a simple answer. My own opinion is that it's a question of common sense, good manners, courtesy and trust. These are constructed as we get to know people electronically, as we "test" them, and as we learn how they can be trusted. The private message system component of EIES is crucial for the conferencing component for many reasons, including clarification, letting off steam, side comments on ongoing issues, etc.

Person A, another aspect of this that disturbs me is your messaging me several times that you didn't "really know me," wanted to get to know the "real me" better, etc. Now, what would you have done with that info, anyway? Person A, you ask Person F to relate to you, accusing Person B of being "reluctant to become involved in our learning about each other." On the basis of the messages following that, can you now understand why they, like I, feel this way? I feel very strongly that the entire issue is a question of trust, and that you have clearly stated, many times, that you neither want nor deserve our trust. If this is "bouncing off each other," it cannot be helped.

C117 CC227 PERSON B 8/ 9/77 2:50 PM

I don't see this as a free speech/free press issue. Rather, for me it has much more to do with trust among people communicating in this electronic wonderspace. Just as I know friends and neighbors whom I can't trust to always be discreet (and so I don't tell them sensitive things), so there are probably people in a cc environment who similarly pass things along that I might not like to see made public. Person A, perhaps I can come to a working compromise. If I clearly label private messages to you as private, will you be willing to keep them that way? Then you don't have to be responsible for figuring out what's confidential and what's not. I would be willing to follow this arrangement with you.

C117 CC228 PERSON A 8/ 9/77 3:23 PM

I am reasonably happy with the arrangement, you don't have to label every msg, just the topic. What bothers me is that the norm EIES is promoting will require that I come to the same understanding with everyone. As I think that information should be generally free, I really would prefer if the understandings would be made the other way around. If I have to make that understood to everyone I meet on line I won't have room in my [directory] description to say anything else about myself.

I don't see this as a matter of trust, to me it is a matter of the cost of information...Person E, I can be trusted when it is clear to me that there is something about the subject which would restrict (as a matter of course) the logical audience to myself. I hope that you understand.

C117 CC230 "ALPHA" 8/ 9/77 4:25 PM

"The norm EIES is promoting" is the only reasonable one to promote. Only some information should be free. I do think, however, that you must make your position clear to everyone you speak to on line.

C117 CC231 PERSON A 8/ 9/77 4:48 PM

Why is it reasonable? What is my position? Why would I want to send copies to everyone, or of everyone's, I speak to on line? And having fully expressed myself, I think that Person E's norm of feeling people out to decide what part of them is public makes the most sense (I think I slightly mangled what she said). For your benefit, if I give you anything I would rather were not public, it's my problem, not yours.

Person B, is there any item of yours which I have entered into this conference which you considered to be based in emotion rather than factual information? I think that it is up to people to speak their own emotion, I can make mistakes.

Come on folks, what's the difference between doing it and admitting that you're doing it? At least by admitting that I am doing it I have gained some idea of when I should not be doing it.

C117 CC233 PERSON C 8/ 9/77 8:21 PM

Actually people the norm you are referring to and that particular section of the booklet was ghosted by Roxanne [Hiltz]; however, I agree with it as it stands in the sense that many new users will not initially realize how easy it is for a message to get circulated around so I would rather see the initial emphasis this way to alert people.

C117 CC240 PERSON D 8/10/77 9:11 PM

I think you will find, Person A, that your recent bullying statements have excluded you from getting any further messaging of significance from most of the other people in this conference. That is too bad, since this is the conference you claim you were given because of your threat tactics. Pyrrhic victory, I'd say. Good bye until the wind changes.....

C117 CC241 "ALPHA" 8/10/77 10:09 PM

I, like Person D, will no longer speak to you, in this conference, except perhaps, and less frequently, through this pen name. Somehow, it makes me feel less vulnerable to your tactics.

C117 CC247 "BETA" 8/11/77 8:41 PM

Hypothesis:
You people are just bored with the range of topics in this discussion now, and you want to migrate to something new and different. (Electronic Casanovas??)

Second hypothesis:
Some of you have felt more free to say very negative things to one another here than you would ever have said face-to-face.

Perhaps Person A's dilemmas were anticipated by Ursula LeGuin in "The Dispossesed." In that book, it's clear that a thoroughly anarchistic society is paradoxically highly dependent upon a very heavy internalization of norms by its members; otherwise you can't trust them to behave socially on their own volition. Norms aren't just stifling; they give predictability.

APPENDIX D: Identities and Role Definitions in Computerized Conferencing

By Elaine B. Kerr

We are concerned with the kinds of interpersonal processes and phenomena that occur in computerized conferencing which correspond to phenomena in non-electronic society and which are unique to the electronic mode. The presence of electronic social forms constitutes the basis of a sociology of the world of electronic group communications. We want to probe where and how the electronic medium may distort or reshape structures, functions, and processes common to other kinds of social interaction -- like mirrors in a fun house -- and we want to explore the consequences.

Electronic social relationships are those in which communications among individuals and groups are electronically mediated. Human communications are assisted and structured by a computer. The Electronic Information Exchange System (EIES) is one such computer-mediated technology from which a social system has emerged.

Unlike conventional social forms, interaction in computerized conferencing is not face-to-face, geographically proximate, or necessarily synchronous. Electronic groups are theoretically and substantively very different kinds of emerging social forms, rather than simply extensions or replications of existing social structures, processes, and interaction patterns in conventional groups and organizations.

This paper is intended to contribute to the morphology of electronic group life by highlighting one practical issue: the implications of the use of pen names for personal identity in electronically mediated groups.

Because written communications are substituted for conventional face-to-face or telephone interaction in electronic groups, standard non-verbal cues (such as smiles, frowns, and other body language) are either replaced by functional equivalents or are unavailable [24]. The pen name capability in computerized conferencing, as demonstrated in EIES, may serve either as a cueing feature or as an identity mask, depending in part on the context and purpose of the specific interaction. New role definitions, self-images, or masks can be deliberately donned, tried on for fit, worn on approval, and exchanged as often as the wearer chooses.

The abscence of non-verbal cues is frequently perceived by new users of computerized conferencing systems as a troublesome barrier to effective communication. The pen name feature, however, can serve in unique ways to partially counter this and other problems.

The pen name feature acts, in part, to counteract the tendency of conventional face-to-face meetings to be ruled by dysfunctional and irrelevant criteria. People are able to communicate in a computer-mediated meeting without reference to their physical appearances or auditory qualities. Ideas and other achieved statuses are relevant to

the written exchange of ideas, rather than ascriptive characteristics over which the individual has no control.

One of the many advantages of computer conferences over face-to-face meetings, which ensues in large part because of the capability of commenting with a pen name or anonymously, is the reduction of social inequality as it affects groups such as minorities, women, and the handicapped, since the user may elect to mask particular status cues. Equally important is the ability to disguise cues irrelevant to professional and scientific dialogue which do exist in general collegial communications, such as age, race, beauty, physical size, loudness of voice, body language, mannerisms, assertiveness, socio-economic status and organizational position. Users may choose to reveal or hide, accentuate or ignore, certain personality, social, and cultural characteristics which would be readily apparent in communication by other media.

Pen names can hide cues which could distract more than enhance the quality of group communications, especially when a group is convened with a mission of scientific inquiry and communication, rather than simple socializing.

The very nature and quality of the contents of communication may undergo major alterations as the pen name assumes over time a unique personality. This personality may or may not reflect its human source, as the user may or may not allow abberant or exaggerated dimensions of his or

her personality to emerge and take shape. Aspects of the self that one might be reluctant to expose to one's professional or social peers may be revealed because of the presence of the pen name option.

Part of the design philosophy of EIES incorporates the user's ability to send messages or enter conference or notebook comments in one of three modes chose: with a signature, a pen name that he or she selects and may change, or anonymously. The three options, in their message format, appear as follows:

```
M 10584    ELAINE KERR (ELAINE,114)    8/ 1/78  7:26 PM  L:1
This is the sample text of a message.

M 10585    "JANE ADAMS"                8/ 1/78  7:27 PM  L:1
This is the sample text of a message.

M 10586    (ANONYMOUS)                 8/ 1/78  7:27 PM  L:1
This is the sample  text of a message.
```

Unconventional configurations, not common to other social forms, are made feasible by the structure of the system.

The possibilities in the message system look like this:

	SENDER		
RECEIVER	Name	Pen Name	Anonymous
Name	Normal Message System	*	*
Pen Name	*	*	*
Anonymous	Planned future possibilities		

Cells noted above by asterisks denote the parameters of concern. Although it is not now possible to address messages directly to specified anonymous recipients, this feature is planned for future implementation, and suggests even more complex and unknown consequences as anonymous-to-anonymous interaction becomes possible. Anonymity, or the masking of identity by the usage of a pen name, is further increased in any of the cells above except the normal message system, as a result of the ability of any user to copy an item received to any other user. In other words, with message passing, the sender of an unsigned item need not have been the recipient of the original item being responded to. Message passing produces anonymous receivers as well as anonymous senders.

These unique patterns can produce certain kinds of attitudes and behaviors which otherwise would not likely

exist. They permit defined lines of thought to be pursued without the necessity of revealing one's identity or unmasking the identity of others. In the EIES public conferences, the receiver of items may choose to remain anonymous by either non-response or unsigned response; in private conferences, however, item recipients cannot easily remain anonymous since conference markers are automatically updated unless the user deliberately changes his or her marker.

Pen names on the EIES system are unique. The first individual to choose one has ownership rights until he or she elects to change it.

Pen names can also be used for tension-release purposes to alleviate overwork and ease the strain of late hours. Yet another function of pen names is to enhance or raise questions about a user's identity and characteristics.

Pen names can be used to foster the unencumbered submission of controversial positions in serious on-line work efforts, although this has not yet been conducted in anything but an ad hoc way.

The pen name feature has also been used for administrative reasons, but again for purposes other than those for which it was originally intended. An administrative use has emerged with a prefix such as (NOW 112) or (AS 902) to indicate recent or impending changes of membership identification numbers. Some users, particularly those who are new, use a

variation of their proper name as a pen name. This is probably a result of confusion between the pen name and the nickname as system identifiers. The phenomenon of shared names constitutes the third aspect of this kind of administrative use. An associate or spouse who shares a membership on the system may use his or her proper name as a pen name to distinguish communications from those emanating from the listed member. An institutional name may be used as a pen name when several people from the same organization share membership with the listed member. Or a guest may be listed by his or her proper name as the host's pen name when on line for demonstration or other temporary purposes. All together, thirteen such administrative uses of pen names were found in a sample listing of 185 pen names on line.

Yet another use of pen names involves masking, deception, or charades in the attempted violation of the system's assignment of unique names to its users -- what one person referred to as "electronic rape." For example, a user under a pen name identification admitted to establishing Roxanne (Control D) Hiltz as a pen name, which would appear as:

ROXANNE HILTZ

To deal with this potential deception by clearly distinguishing pen signatures from real signatures, a design change was implemented to label pen names in this form:

"JANE ADAMS"

The pen name and anonymity features are among the elements of informality deliberately built into the system to attempt to overcome the impersonality and coldness that many associate with computers. The design assumption is that social needs are real, legitimate, and necessary for task achievement. Features such as pen names promote informal and less serious exchanges, and in this way can function as electronic substitutes for the pre-meeting chatter, coffee breaks, or cocktail hour. Other tension-release mechanisms that have emerged on line include informal conferences, both planned and unplanned on-line "cocktail parties," and a temporary encounter-type session.

Pen names may serve as a tool for the temporary redefinition of self. They reflect changing attitudes, values, and cognitive structures, and permit new kinds of role-playing and symbolic behavior, especially by experienced and sophisticated users of the system. (New or infrequent users are unlikely to be sufficiently familiar with the system's mechanics to fully explore these kinds of possibilities.) But the mask may be torn off and the true identity exposed. One likely consequence is that the pen name will be changed, and attempts to conceal the new name may be more strenuous than before.

The masking of identity is more difficult to sustain with the usage of pen names than by anonymity, since the pen name can assume a more focused and clear identity over

time. (For example, in the Encounter Conference, "ALVEY SINGER" emerged as the trouble-maker, "GERTRUDE MCFUZZ" as the feminist, and "THE EIES COMPUTER" as the threatening authoritarian.)

We can make guesses about the author of a pen-named item, but must realize that, for example, a male might deliberately choose a female pen name, or vice versa, to avoid identification. We can make suppositions about the circumstances under which particular pen names are used, but must remember that the pen name may stay constant while the context of its usage changes.

We would like to know the varied effects of pen name usage on the different audiences addressed. Does receiving a pen-named item make it more likely that the reader will respond at all, and that the response will in turn be signed with a pen name? It would be useful, but is not possible, to examine the proportion of time in each conference that members utilized their pen names or one of the alternates. Does the use of pen names contribute to the frivolous waste of electronic space, as some might argue, or does it instead serve as a valid tension-release mechanism?

We do not know, and cannot simply determine, given the protections for user input built into the system, the answers to such intriguing questions as:

- How are pen names chosen?
- What factors influence their choice?
- How frequently are they used?
- In what contexts are they used, discovered, and changed?
- The characteristics of those who use the pen name feature compared with those who do not
- How secure users feel using pen names compared with anonymity

It would be useful to investigate changes in the kinds of pen names chosen over time. The nature of such trends in content could clarify the uses to which the pen name capability is applied. We might be able to note and predict, for example, that certain kinds of pen names tend to be chosen by certain kinds of users in specific contexts. The relatively small time period under review, the likelihood that only a small proportion of users have yet made full and frequent use of their pen name capability, and the relatively small but growing system sophistication of these users, however, makes this line of inquiry now impossible. (Users have been questioned as to their pen name habits, but this request was not made to all users of the system, and not all who were queried did respond.)

Two listings were constructed on pen names in use on the EIES system: one yielded 141 names for the almost 400 users then on line, and the second, culled from a review of three

conferences, produced 44 additional names. These lists do not always tell us if the name has ever been used, the frequency of its use, or its duration. And we cannot, of course, match pen names with specific users. Although some of the identifications are known to us, they must remain confidential. We have on-line access to some but not all of the communications with pen name signatures.

Of the 185 pen names accumulated, twelve mutually non-exclusive and overlapping categories were discernible.

CLASSIFICATION	EXAMPLES	NUMBER
Male	Michael, Masked Man	39
Female	Madame Curie, Elizabeth	15
Passive or Meaningless	Me, None	31
Authoritarian, Expert, or Assertive	Consultant, Resource	26
Humorous	Baron Wed Wabbit, Chuckles	26
Mythological or Fantasy	Thor, Merlin	11
Science Fiction or Space	Spaceman, R2D2	11
Entertainment	Woody Allen, Elvis	10
Literary or Classical	Christopher Marlowe, Falstaff	8
Foreign	Bolshoi Brat, Catherine the Great	6

Computer references	The EIES Computer, The Micro-Code Maniac	5
Unknowns and Problems	Janem, Imjed	37

An analysis of the comparative length of items in two conferences was performed. The first, Conference 119, was a private, informal, leaderless, and unstructured conference entitled "Encounter Session." Twenty-three conferees produced 230 comments between August 1977 and June 1978. The second, Conference 1005, is the "Wisdom" public conference, open to all members of the EIES system. An unknown, but probably large number of participants, entered a total of 112 comments since October 1976. This, too, is a leaderless, informal, and unstructured conference. Compared with Conference 119, Conference 1005 had fewer themes, and the topics which did emerge seldom achieved sustained discussion.

CONFERENCE 119

Length	Signed	Pen Name	Anonymous	Total
1-5 lines	51 (46%)	59 (76%)	35 (74%)	145 (63%)
6-49 lines	59 (54%)	19 (24%)	7 (16%)	85 (37%)
TOTALS	110 (100%)	78 (100%)	42 (100%)	230 (100%)

CONFERENCE 1005

Length	Signed	Pen Name	Anonymous	Total
1-5 lines	10 (34%)	26 (65%)	28 (65%)	64 (57%)
6-49 lines	19 (66%)	14 (35%)	15 (35%)	48 (43%)
TOTALS	29 (100%)	40 (100%)	43 (100%)	112 (100%)

Conference 1005 has a higher proportion of unsigned items than Conference 119, but this is a consequence of the heavier use of anonymity there. The frequency of pen name usage is essentially the same in the two conferences.

In Conference 119, although almost half of the entries are signed, pen names are used almost twice as often as anonymity. In Conference 1005, the distribution is much more even.

Both conferences have a preponderance of relatively short items, which is not surprising in view of their informal nature. Also in both, the signed items are longer than the unsigned. This suggests two possibilities: that those going to the trouble of typing in longer conference comments wish their efforts to be recognized, or that those choosing to mask their identities with either pen names or anonymity deliberately keep their items short in an effort to avoid detection through use of identifiable syntax or word choice.

Of the shorter items, a higher proportion are signed in Conference 119 and anonymous in Conference 1005.

NOTES

1] In addition to CB radio, social observers, of course, have noted the use of "anonymity" in mob behavior and in the masking function of the automobile; and the distressignly disastrous outcomes of such behavior.

2] See Price (1963). One recent paper on a nuclear physics experiment was co-authored by no less than 79 people. Some delphi studies and similar structured group exercises could be said to have been written by literally hundreds of co-authors. The authors listed for the published results of such exercises might more properly be termed editors or facilitators. A recent publication derived from EIES (Turoff et al. 1978) was edited by seven people who organized their own contributions and those of 28 other people who had contributed to three computerized conferencing groups.

3] Illegal entry to computerized data files and processes is an omnipresent threat to the privacy, confidentiality and anonymity functions of all computerized systems. The subject has been treated extensively elsewhere, and lies beyond the scope of this report which discusses these matters mainly in terms of those authorized to use the computerized conferencing system.

4] By definition it would seem that censorship in a computerized conferencing system would disallow members to maintain privacy, confidentiality or anonymity. A conferencing system could be maintained without these modes of use and expression, but most of the applications discussed here could not be obtained.

5] See, for example, Kuhn (1970) and Storer (1966).

6] The sanctity of this relationship was underscored by the conviction of John Ehrlichman for authorizing the illegal seizure of Daniel Ellsberg's psychiatric records.

7] A full discussion of the appropriate statutes and regulations can be found in the report of the Ad Hoc Committee on Privacy and Confidentiality (1977).

8] A comprehensive review of results obtained under differing degrees of confidentiality and anonymity can be found in Deutscher (1972).

9] The technique was developed and used by the American Institute of Public Opinion (the "Gallup Poll"). The analogy to election anonymity and terminology is so strongly embedded that to this day Gallup Organization and other Princeton-based researchers commonly refer to survey questionnaires as "ballots."

10] This technique most commonly is used in employee relations surveys to forestall common fears that management will be able to trace opinions back to disgruntled employees. The picture of a manager seeking to determine the identity of the author of a critical message in the company suggestion box has been long a favorite of cartoonists.

11] See Warner (1965).

12] A discussion of the most recent cause celebre in this vein appears in Dickson et al. (1977).

13] Telephone conferencing has been employed only very rarely in the focus group mode, and to the author's knowledge has not been evaluated systematically. It is assumed that a telephone conference focus group would present considerable mechanical, moderating and voice-cueing difficulties.

14] Reliable statistics on the comparative incidence of delphi and focus group surveys are not available, but it is the author's estimate that in the United States focus groups probably outnumber delphi studies by a margin of at least a thousand-to-one.

15] A full discussion of the probable future use of constraint models in computerized conferencing appears in Scher (1977).

16] See Kahn (1967) for examples of real conflict situations, and Staff of Strategy & Tactics Magazine (1977) for exposition of the history and current practices in conflict simulation gaming.

17] The author has observed that new EIES members typically enter their credentials in initial directory listings, but that as they gain experience with the new medium, credential information gradually is supplanted by descriptions of topical interests.

18] An interesting summary of current research findings on the potential biasing effect of personal appearance may be found in Bennetts (1978).

19] Even when members use their given names, in those cases where a name such as Robin is encountered, those not previously acquainted with the member may not always know if the member is male or female. Although evaluative research and experimentation has not been undertaken on the subject, it would seem, and has been reported anecdotally, that computerized conferencing offers women a forum in which sex discrimination is not encountered to the extent that it may be met in more conventional environments.

20] In general, cueing anonymity could be of particular advantage to the physically handicapped or deformed person. The attention directed towards the handicapped, real or imagined, could sometimes be as debilitating as the handicap itself.

21] This discussion of collections is based upon the specifications developed by Whitescarver and Turoff (1978).

22] This statement appears in Turoff and Johnson-Lenz (1977), but was written by S. Roxanne Hiltz.

23] A more complete listing of off-line functions and associated problems and opportunities appears in Bezilla (1977).

24] A more thorough discussion of cue-emitting and cue-searching in computerized conferencing will be given in Kerr and Bezilla (1978).

BIBLIOGRAPHY: Referenced Sources

American Statistical Association.
1977 "Report of Ad Hoc Committee on Privacy and Confidentiality." Statistical Reporter, 77-9:373-398.

Bennetts, Leslie.
1978 "Beauty Is Found To Attract Some Unfair Advantages." The New York Times, March 18, 10.

Bezilla, Robert.
1977 "Off-Line Activities." Hiltz, S. Roxanne, Org. Applications and Impacts Conf. 72 (CC283-285), EIES, Newark: New Jersey Institute of Technology. Reprinted in Turoff et al. (1978) as "Off Line Activities: Technology, Design and Policy Issues," 89-91.

Deutscher, Irwin.
1972 "Public and Private Opinions: Social Situations and Multiple Realities." In Saad Z. Nagi and Ronald G. Corwin, Eds. The Social Contexts of Research. New York: Wiley-Interscience.

Dickson, John P. et al.
1977 "Invisible Coding of Survey Questionnaires." Public Opinion Quarterly, 41:1, 100-106.

Diffie, John P. et al.
1976 "New Directions in Cryptography." IEEE Transactions on Information Theory, November.

Gardner, Martin.
1977 "A New Kind of Cipher That Would Take Millions of Years To Break." Scientific American, August, 120-124.

Hiltz, S. Roxanne.
1975 "Communications and Group-Decision Making: Experimental Evidence On the Potential Impact of Computerized Conferencing." Research Report No. 2, Computerized Conferencing and Communications Center, New Jersey Institute of Technology.

Hiltz, S. Roxanne and Murray Turoff.
1978 The Network Nation: Human Communication Via Computer. Reading, Mass.: Addison Wesley.

Kahn, David.
1967 The Codebreakers. New York: The MacMillan Company.

Kerr, Elaine B.
1977 "Pen Names." M26693. July 26; 5:02 PM. EIES, Newark: New Jersey Institute of Technology.

Kerr, Elaine B. and Robert Bezilla.
1978 "Cue-Emitting and Cue-Searching in Computerized Conferencing." Forthcoming.

Kuhn, Thomas S.
1970 The Structure of Scientific Revolutions, Second Edition. Chicago: University of Chicago Press.

Merton, Robert K.
1957 Social Theory and Social Structure, Revised Edition. Glencoe: Free Press.

Price, Derek J. de Solla.
1963 Little Science, Big Science. New York: Columbia University Press.

Rivest, Ronald L. et al.
1977 "On Digital Signatures and Public-Key Cryptosystems." Laboratory for Computation Science, Massachusetts Institute of Technology, Technical Memo 82, April.

Scher, Julian M.
1976 "Communication Processes In The Design and Implementation of Models, Simulations and Simulation-Games: A Selective Review and Analysis, From the Vantage Point of Computerized Conferencing." Research Report No. 4, Computerized Conferencing and Communications Center, New Jersey Institute of Technology.

Staff of Strategy & Tactics Magazine.
1977 Strategy & Tactics Staff Study Nr 2: Wargame Design; The History, Production, and Use of Conflict Simulation Games. New York: Simulations Publications.

Storer, Norman W.
1966 The Social System of Science. New York: Holt, Rinehart, and Winston.

Turoff, Murray et al.
1978 "Research Options and Imperatives In Computerized Conferencing." Research Report No. Ten, Computerized Conferencing and Communications Center, New Jersey Institute of Technology.

Turoff, Murray and S. Roxanne Hiltz.
1977 "Computerized Conferencing: A Review and Statement of Issues." In Martin C. Elton et al., Eds. Evaluating New Telecommunications Services. Proceedings of a Symposium Held at Bergamo Italy, September 5-8, Sponsored by the NATO Special Program Panel on Systems Science. New York: Plenum, 1978.

Turoff, Murray and Peter & Trudy Johnson-Lenz.
1977 "How To Use Electronic Information Exchange System." Research Report No. 7, Computerized Conferencing and Communications Center, New Jersey Institute of Technology.

Warner, Stanley L.
1965 "Randomized Response: A Survey Technique for Eliminating Evasive Answer Bias," Journal of The American Statistical Association, 60:63-69.

Wellman, Barry.
1978 "Masks and Pens." M18944. March 1; 10:54 AM. EIES, Newark: New Jersey Institute of Technology.

Whitescarver, James and Murray Turoff.
1978 "Material Collection." Specifications Conf. 95 (CC67-75). April 8; 3:52 PM. EIES, Newark: New Jersey Institute of Technology.

Zuckerman, D. and R. Horn.
1973 The Guide to Simulations/Games for Education and Terminals. Hicksville, New York: Research Media.