NBSIR 79-1793

Privacy As Information Management: A Social Psychological and Environmental Framework

Stephen T. Margulis

Center for Building Technology
National Engineering Laboratory
National Bureau of Standards
Washington, D.C. 20234

September 1979

U.S. DEPARTMENT OF COMMERCE
NATIONAL BUREAU OF STANDARDS

NBSIR 79-1793

PRIVACY AS INFORMATION MANAGEMENT: A SOCIAL PSYCHOLOGICAL AND ENVIRONMENTAL FRAMEWORK

Stephen T. Margulis

Center for Building Technology
National Engineering Laboratory
National Bureau of Standards
Washington, D.C. 20234

September 1979

U.S. DEPARTMENT OF COMMERCE, Juanita M. Kreps, *Secretary*

Luther H. Hodges, Jr., *Under Secretary*

Jordan J. Baruch, *Assistant Secretary for Science and Technology*

NATIONAL BUREAU OF STANDARDS, Ernest Ambler, *Director*

TABLE OF CONTENTS

	PAGE
ACKNOWLEDGEMENTS	iv
1. INTRODUCTION	1
1.1 Background	1
1.2 Status of Current Theories of Privacy	3
1.3 The Scope, Aim and Organization of the Report	3
2. PRIVACY AS INFORMATION MANAGEMENT: AN INTRODUCTION TO A FRAMEWORK	5
2.1 What is Privacy?	5
2.2 Information and Communication	7
2.3 On the Loss of Privacy	8
2.4 Personal Control	10
2.5 Costs	13
2.6 Boundary Regulation	14
2.7 The Physical Environment	16
2.8 Summary	20
3. REFERENCES	21

ACKNOWLEDGMENTS

The author wishes to thank John Archea, Fred Stahl and George Turner for helpful comments on an earlier draft of this report and Tracey Kistler for the preparation of this report.

1. INTRODUCTION

1.1 BACKGROUND

An objective of environmental design research at the National Bureau of Standards (NBS) is the production and application of knowledge leading to more useful buildings. Buildings can be made more useful, it will be argued, by more adequately providing for the privacy of occupants and users. From a scientific perspective, good theory should help such an enterprise because good theory creates understanding of phenomena and guides their measurement and application. This report proposes a social psychological and environmental framework for constructing a theory of privacy applicable to the built environment.

If we limit ourselves to privacy and buildings, a review of the relevant literature leads to the conclusion that privacy is an important, sometimes a critical, factor in a number of settings including: offices (Justa and Golan, 1977; "The Trouble with Open Offices," 1978); hospitals (Cammock, 1975; Thompson and Goldin, 1975; Veterans Administration, 1977); prison (Filipczak, 1973); banks (Prather, 1972); and in what may be the most studied setting with regard to privacy, housing.

Housing occupants, both in their choice of housing ("What Buyers Say They Want in Housing in 1978," 1978) and in their evaluation of it (Cooper, 1975; Francescato, Weidemann, Anderson and Chenoweth, 1975; Sanoff and Sawhney, 1972) mention privacy considerations. As a rule, being able to have and maintain privacy is evaluated favorably and not being able to obtain privacy or having one's privacy violated is evaluated unfavorably. Designers of housing share occupants' belief that privacy is important and should be supported by the design of occupants' housing and sites (Chermayeff and Alexander, 1965; Churchman and Herbert, 1978).

Studies of housing that discuss the role of privacy in occupant satisfaction raise a number of points which theories of privacy should consider.

1. Privacy requirements appear to be universal, although the forms they take are culturally variable (Altman, 1977; Rapoport, 1969).

2. In studies in Western societies, a large number of housing and site features have been associated with privacy. These include plumbing, windows, walls and fences, and the layout, location and orientation of a dwelling (Cooper, 1975; Francescato et al., 1975; Mautz, n.d.).

3. A particular environmental feature (e.g., a fence) may be associated with more than one situational attribute (e.g., privacy, security, safety). In some cases, the feature can support the different attributes; in other cases, the attributes conflict (e.g., Cooper, 1975).

4. Visual and auditory privacy are common foci for comment. (It is likely that in settings where odors can be significant threats to personal privacy, such as in hospital, this foci would be more common.)

5. Although current housing research has demonstrated an association between the built environment and occupant's comments about privacy, the relationship has yet to be explained. That is, how does the built environment affect behavior?

Two specific examples will tie these considerations to building usefulness. In both examples, occupant satisfaction is the indicator of utility. The first example, involving visual privacy, is from a Swedish study ("Convenience versus Privacy," 1973) which compared opinions of occupants of apartments in different types of housing. Occupants of balcony-access housing had privacy problems. In this housing, apartments are entered from balconies that ran the length of the buildings. The balconies are part of the circulation system for the buildings. In these apartments, the kitchens were the only room to face the balcony. Kitchen windows created a keenly felt lack of privacy. The households that felt this loss of privacy (nearly half of all interviewed households in these buildings) expressed little enthusiasm for the concept of balcony-access living, a design concept that, at the time of the study, had been receiving increasing attention in Sweden. Although the simple expedient of screening the lower half of the kitchen window considerably reduced the complaints about visual intrusions by passers-by, this solutions also impaired the view and reduced the admission of sunlight into the kitchen, two new undesirable consequences. Thus, the location of the kitchen window can be regarded as a design decision that reduced the utility of these buildings.

An American study (Cooper, 1975) of families in low-cost row housing provides the second example. The issue, here, is the consequences of design and construction decisions on auditory privacy of occupants. The housing was wood-frame construction, with party walls of staggered studs separated by rock wool bats. To produce a variety of interiors, the units were designed with overlapping room arrangements, so stairs in one unit ran past the kitchen of another and a bedroom in one unit was over the living room of another. As a result, for many occupants, noise was a serious problem. For example, tenants found themselves overhearing quarrels in other apartments they did not want to hear. Moreover, occupants recognized that what was happening in their own apartments could be heard by their neighbors. The lack of auditory privacy was a source of considerable adverse comment, both as a source of embarrassment and as an annoyance. For this occupant group, building design and construction decisions created sound transmission problems that reduced the utility of these buildings. A good theory of privacy could have been a means of addressing and resolving the privacy problems found in this and in the Swedish studies.

1.2 STATUS OF CURRENT THEORIES OF PRIVACY

During the 1970's, there have been signs of increasing interest among behavioral scientists and environmental design researchers in privacy (Margulis, 1975, 1977c). This interest reflects, in part, a desire to understand the relationship between buildings and people, and to more completely explain the nature of social relationships. The interest undoubtedly reflects, too, a growing citizen and governmental concern with actual and potential abuses of privacy (Margulis, 1977b).

Has this interest in privacy resulted in good theories of privacy? An answer to this question rests on two assumptions. First, privacy is an important, if not central, socioenvironmental concept (Altman, 1975; Canter and Kenny, 1975). Second, understanding privacy requires an adequate explanation of how the physical environment determines, influences or provides support for behavior. Unfortunately, not all who endorse the first assumption have tried to link their ideas about behavioral aspects of privacy with conceptually adequate representations of the nature and functioning of the physical environment (Levy, 1976). Consequently, it is concluded that current theories of privacy are, for the most part, insufficiently developed for fully understanding privacy and, consequently, are of only limited use in solving practical environmental problems involving privacy (Margulis, 1977a).

1.3 THE SCOPE, AIM AND ORGANIZATION OF THE REPORT

This report is part of a continuing attempt to create a framework within which a theory of privacy can be developed. It is unlike many of the major theories of privacy (e.g., Altman, 1975; Laufer and Wolfe, 1977) that have been developed in the last decade which specifically try to bring order to the many meanings of privacy found in the technical and nontechnical literature (Margulis, 1977a). By contrast, the framework is narrow in scope. It limits privacy to certain conditions of limiting and protecting information. Other conditions of information management, such as those associated with secrecy (Warren and Laslett, 1977), espionage (Wilsnack, in press) and censorship (Margulis, 1977a), presently fall outside of the proposed framework. Furthermore, unlike many other current theories of privacy, the present framework strongly endorses the position that a complete understanding of privacy requires a complete understanding of the nature and functioning of the objective physical environment. In all, this effort at concept development is predicated on the belief that a theory of privacy and its associated measurement methodologies, based on the proposed framework, can be of potential use for addressing privacy requirements. The resulting knowledge, in principle, can be applied to housing and site design decisions, construction decisions, building management decisions, and to regulatory and zoning decisions affecting buildings.

The aim of this report is to introduce, briefly and nontechnically, some of the ideas about privacy that the author has been developing. This report does not attempt to systematically review, summarize or critique particular theories of privacy or the research literature on privacy,

other than the material appearing in Sections 1.1 and 1.2. Reviews of theory and research can be found in Margulis (1975, 1977c).

Organizationally, the report introduces behavioral aspects of privacy in the early sections (Section 2.1-2.6) and environmental considerations in a later section (Section 2.7).

2. PRIVACY AS INFORMATION MANAGEMENT: AN INTRODUCTION TO A FRAMEWORK

2.1 WHAT IS PRIVACY?

The essential focus of this analysis of privacy is the strategic and tactical management of information, specifically information whose loss would have costly consequences for the person who is the target of the information. Such information will be called "personal" or "private" information because the person, P, the target individual in the analysis, feels he or she has a claim to the information (i.e., feels it rightfully belongs to him/her). It is assumed that if there is no such claim, there is no issue for P with regard to informational privacy. However, one seldom finds a direct test of this assumption. Rather, if there is intentional protection of information and intentional control of access to the information, and if there are stressful reactions to unwarranted and unwanted access to the information, these serve as clues to asserting that the information is regarded as personal and requires management. Put another way, the basic question for P is: Who knows or could know about X (the private information of P, which includes its linkage with P), and what are the consequences to me (P) if a particular Other (other person), O, knows about X (or P-X, its linkage with P), now or in the future?

The question poses three problems for P to consider. P's response to each of these problems will determine whether information management is an issue and, if it is, the nature of information management. The three problems are:

1. Deciding who should and who should not know about X. This decision is built on a number of antecedent judgments and evaluations of one's self, of the information, of the setting, of the potential recipient, etc. For example, there are clearly those with whom P would want to share private information and others that P would clearly want to exclude. However, there is a third class: people whose presence during a private event is a matter of indifference to P. Such persons are not regarded by P as threats to information management. Consequently, when these persons are physically present during a private event, they may be treated by P as being "not present" (Goffman, 1959). Examples of such "non-persons," to use Goffman's (1959) term, are infants, slaves and servants, and service workers, such as simultaneous translators and court stenographers, whose effectiveness is enhanced when they are treated as "not present."

2. Having the competence to control one's communications so that those who should not know about X or P-X do not learn about it. Competence implies the ability or skill, of both the sender and receiver of information, to each control his/her own response to internally or externally generated messages, and to encode and decode messages. This means, in part, that one person's (P's) ability to "keep" or control a "secret" is measurable against another person's (O's)

ability to "read" or gain access to that "secret". In turn, O may now be measured by O's ability to keep his or her successful breach of P's "secret" from P. Theoretical statements about competence presume that P wants to control certain situations and settings. It is assumed that competency is not uniform across persons, stages in one's life cycle, one's internal states, tasks (particularly encoding versus decoding messages), and classes of content. Communication refers to the content and flow of information from P to others and from those recipients to additional others (through any and all channels of communication).

3. Managing one's failure to control information as well as managing the consequences of having information (X or P-X) fall into the possession of those whom P believes should not have it.

An example will illustrate these three problems. Imagine a hungry child enticed into the kitchen by the thought of a delicious cookie, a forbidden treat. The child knows his parents disapprove of snacks, especially before mealtimes, and that they will punish him for eating such snacks. [This illustrates Problem 1.] Nevertheless the child eats the cookies greedily. Although unseen and unheard, traces of evidence remain: crumbs on the floor and tell-tale food stains about the mouth. Confronted by his parents, the surprised child stares wide-eyed but otherwise remains silent. The evidence and his response to the interrogation -- a pattern of responding which the parents believe is associated with wrong-doing -- plus the child's sluggish appetite during dinner, reinforce the parents' suspicions. The child's silence in this context is regarded as a social equivalent of a "no contest" plea. [This illustrates Problem 2.] The child is punished. [This illustrates Problem 3.]

Thus far, we have described and illustrated privacy. However, a formal definition is in order. Privacy refers to behaviors of the individual that are intended to or that express or test the individual's competence to control the flow and/or content of information transmitted to a specifiable audience (network) of others. This formal definition of privacy refers to information to which a person (P) believes he or she has a legitimate claim; the person believes the information belongs to him or her. It might be thought of as "cognitive property." This claim (by P) is either exclusive ("I and no one else can make a claim to this information"), or shared ("Others have or can raise a legitimate claim to this information"). In either case, it is a posited characteristic of this claim that P will regard the withholding or transmission of the the information as a matter of P's voluntary assent.

There are at least three bases for a claim over information. One basis is being the creator of the information. This would include one's own thoughts and ideas or one's evaluation of or thinking through the thoughts or ideas of others. A second basis is a normatively defined and recognized relationship between a person (P) and information (X, P-X). One's name and other indicators of personal identity are examples. A third basis is the obligations of P toward those who have

shared private information with P. Examples are confidences which are shared because of social bonds of love or trust, or through necessity. Information shared of necessity includes revelations by the penitent to the priest, by the client to the lawyer, and by the patient to the physician. Personal obligations built on social bonds of love and trust are the reasons for protecting personal "secrets" and confidences; personal obligations built on legal and professional requirements are often the reasons for protecting "secrets" and confidences shared of necessity.

2.2 INFORMATION AND COMMUNICATION

The terms "information" and "communication" are used broadly. Many facets of observable human behavior are regarded as potentially informational and as communicable. Thus, communication is not limited to exchanges that are spoken or written, although these are important, but communication extends to dress, physical appearance and health, use of space, paralanguage, and kinesics ("body language").

A communicative act (communication), formally speaking, is a transmission of information from a source to a recipient.[1] ("Transmission" is used as a synonym for "communicative act" here.) Information, in formal terms, is that which is discriminable, classifiable, or meaningful (particularly for the receiver of the information). Because this may seem far removed from the use of the term thus far, we will define "information" informally as anything that makes a difference to or which is meaningful to a communicator or recipient.

One class of information, called "personal" or "private" information, is information to which the person lays claim. It is a characteristic of private information that even after it has been transmitted to recipients, P may still regard it as "private" (i.e., it is still P's "cognitive property"). Consequently, P may feel that recipients have an obligation to P to protect the private information which P has shared with them.

Types of information that segments of contemporary Western societies might treat as "private", at one time or other during their lives, include the following.

Health: includes mental and physical health, past and present; illness and treatment, medicines taken, prosthetic devices; disabilities, disfigurements, and other health-or-body-related stigma.

Sexuality: includes sexual practices, values, interest; contraception; sexual dysfunctions; association with pornography and sexually stimulating material; all social deviance of a sexual nature.

---

[1] This analysis draws on Newcomb (1953, 1959).

Social deviance and illegal acts: includes criminal acts, or acts that the person or others might regard as criminal, immoral, taboo, or unethical; criminal records, arrests without prosecutions.

Legally protected communications: includes personnel files, credit files; communications with lawyers, physicians, ministers that are legally protected; corporate "secrets" and their management (business-related secrets) as well as classified documents. Key is that the communication between person and other is legally protected and legally limited (defined).

Demographic or social class information: includes all references to income and personal/family finances, education, ethnicity, religious affiliation, occupation, residence where this information of itself is hidden because of what it tells about the person.

Psychic preparation and psychic repair: any acts that permit the person to get his or her emotional, cognitive, or behavioral array in order; preparation for a public display especially following stress or grief; tasks initially performed or developed in private in anticipation of a public presentation.

Personal affiliations and associations: persons or groups with whom one affiliates, past or present, especially unpopular, stigmatized, rejected persons or groups.

Self-defined or socially-defined embarrassments, limitations, and weaknesses: the "Candid Camera" class of situations that might be embarrassing; minor idiosyncratic problems that people hide.

2.3 ON THE LOSS OF PRIVACY

The proposed emphasis on both the person, P (the target of personal information), and on the recipients as potential communicators raises two theoretical points upon which an analysis of a loss of privacy is based. One point focuses on the communicator of personal information. A communication by P to certain recipients must be distinguished from communications by those recipients to others. Furthermore, the acceptability of recipients as communicators and the propriety of specific transmissions by recipients to yet additional recipients must be considered from P's perspective. A second point addresses the acceptability of recipients of P's information to P, regardless of who has transmitted it.

These points have resulted in distinguishing an invasion of privacy from a violation of privacy -- both of which are losses of privacy. When an unacceptable person is an audience to a transmission by P of private information about P, this is an invasion of privacy. A violation of privacy is the unwarranted presence (from P's perspective) of a person during a transmission of private information about P by a recipient to others. The violation of P's privacy occurs when initially acceptable or unacceptable recipient transmits personal information about P to

someone whom P does not regard as acceptable. This holds even when the individual unacceptable to P is acceptable to the recipient-communicator and is invited to share the information. A violation of privacy means that P has failed, for whatever reason, to control successfully the dissemination of his/her own private information. Within this framework, there can be invasions with or without violations and violations with or without invasions. To illustrate both an invasion and a violation, imagine that a husband and wife are keeping confidences from their children. The presence of one of their children at such an exchange would constitute an invasion of privacy. A discussion of this exchange by that child with a brother or sister would constitute a violation of privacy.

This analysis assumes that private information tends to be shared. Sharing can be represented as a communication network which is extended over people, space, and time. In principle, this network should completely and objectively depict the flow of information to and from all the points (persons) in the network. It should distinguish between transmissions that have and that have not resulted in a loss of privacy for whatever reasons. It is recognized that the reasons for the flow may or may not be intentional, planned, or justified, and that the flow may or may not conform with the desires of the target person.

There is an important corollary of loss of privacy as considered. The actual audience (i.e., those who obtained X, or know P-X) and the audience as it is believed to be by P may not correspond. The lack of correspondence may arise from P's ignorance about the true state of affairs, or from defensive or adaptive mental states which distort perceptions of the communication network. Because such discrepancies can affect social behavior, it will be necessary, in theory and in research, to represent both of P's audiences -- the perceived audience and the actual.

The framework distinguishes two ways in which potential audiences can affect privacy behaviors. First, environmental settings create opportunities for persons who are present or who could come on the scene to invade or violate P's privacy (see Section 1.7). Second, P may consider how future audiences might react to current information about P. Wolfe and Laufer (1975) point out that present day information storage and retrieval technologies make future access to current information easy, at least in principle. They note, for example, that as opinions change over time, previously legitimate or socially acceptable information may become illegitimate and unacceptable, thus a source of vulnerability if future audiences gain access to the information. An example illustrates this point. Women graduate students, who participated in an inadequately managed encounter group, discovered that their admissions of sexual interests and experiences before the group later became a basis for sexual propositions and harrassment by certain male participants and other males who gained unwarranted access to the group discussion. Conversely, information that creates vulnerability in the present may become benign in the future. For example, American women who pressed for their right to vote were, at one time, held in low regard. In time,

this association ceased to be an issue. Thus, the individual must cope with time-linked uncertainty as one aspect of the exercise of personal control.

Not all losses of privacy require inordinate skill or effort in managing the loss. Losses of privacy studied by experimental social psychologists, for example, tend to involve relatively low costs (Berscheid, 1977). More potent examples are found in letters to Ann Landers and Dear Abby. No doubt it is the potent implications of these letter for their writers that is the reason why they are published anonymously.

2.4 PERSONAL CONTROL

Most contemporary behavioral theories of privacy emphasize that privacy involves or depends upon one's competence to control and understand personal transactions (Margulis, 1975, 1977b). The present theory is no exception. To illustrate the role of personal control: P is more likely to speak openly if P can limit his audience to personally acceptable recipients, and if P is able to select or plan a physical setting that makes an invasion of privacy unlikely. If these conditions are not met, then P, as an expression of his/her competence, might modify the form, content, or timing of a message. Thus, bilinguals who switch languages to exclude others who are present from understanding what is being said are modifying (controlling) the form of the message. Lying and deception also modify message form or content in order to protect certain information. Thus, evaluating situations and settings and, correspondingly, evaluating the form, content, or timing of a message are all aspects of one's competence to control communications.

The framework's approach to personal control draws on the analysis by Johnson (1975). Briefly, Johnson (1975) argues that

> there are at least four stages in the causal chain from awareness of a need state to need satisfaction during which people may influence their outcomes. Starting with the first stage, people may choose their outcomes...; next, they may select their behaviors...; at the third stage they may control the outcomes themselves by exercising those behaviors...; and finally, at the fourth stage people may evaluate and interpret their outcomes.... (p. 85)

He discusses these four stages with respect to the direct versus indirect relationship between a behavior and its outcomes, which he calls direct control and indirect control, respectively. According to Johnson (1975), privacy behavior can indirectly or directly control the flow or content of information to specifiable audiences. Direct control represents the behaviors that attain an intended outcome; indirect control creates the conditions that facilitate behaviors resulting in direct control. If making the manifest content of a message inaccessible to all but a designated audience is P's intent, then encrypting the message is an

example of direct control, and the decision to encrypt rather than use other strategies and the selection of an appropriate algorithm are both examples of indirect control.

These are two cases to which Johnson's analysis of personal control would be applied. First, the prototypical case, is P's competence to control information that has been shared (with P or by P) or that could be shared with yet additional others (by P or O). The case is prototypical because humans are social beings and sociality builds upon and also results in sharing of personal information. Typically, self-disclosures are reciprocated. If disclosure creates vulnerability, then trust and affection are social mechanisms for reducing vulnerability through the creation of protective attitudes. That is, sharing creates a basis for tailoring one's protection of another to known (exposed) sources of vulnerability (Kelvin, 1977). Put in terms of vulnerability, sociality is associated with sharing, and sharing means that absolute control is lost. However, through reciprocal disclosures, each person gains a degree of control over the other since each has made himself/herself vulnerable.

Second, as a special case, is P's competence to control personally the information which P would like to keep in his or her sole possession. This special case requires P to match his or her own competencies (skills) against the competencies of O to overcome P's suppression, concealment, or deception, and hence to decode any "informational leakages" that P provides.

The analysis of personal control also must handle two major ways of communicating private information: selective affiliation and selective communication. Selective affiliation is the tailoring of an audience in a setting to "fit" a communication. The secret society which forbids the revelation of its secret rituals to nonmembers is one example. Another example, recognized by the law, is the privileged communication (e.g., lawyer-client, physician-patient, priest-penitent communications). Selective communication is the tailoring of a communication to an audience in a setting. Examples include an adult spelling "private" messages to another adult when their children are present, multilinguals shifting to a language which is (hopefully) unfamiliar to those they wish to exclude, or the military using cryptological procedures to encode messages. Put another way, selective affiliation refers to P's belief that the audience and setting for a communication are adequately understood and controlled. As a result, P can make the revelation. Selective communication refers to control over message content, including refraining from communication, when P considers his/her personal control over the audience and/or setting to be inadequate. This analysis of privacy implies that, for P, privacy is not a matter of degree or level, that is, of having too much or too little privacy (cf. Altman, 1975). Rather, P's evaluation of his/her privacy is qualitative: "I have successfully managed information" or "I have not" or perhaps "I am unsure." However, the effort exercised to obtain or maintain privacy may be treated as a matter of degree by the person. A second implication of this position is that mechanisms for exercising personal control are governed by goal-oriented concerns and are modified or shifted to assure movement toward

an unexpected or desired goal. However there is no definitive list of mechanisms for limiting and protecting personal information (Altman, 1975; Laufer and Wolfe, 1977). Rather a variety of historical, cultural, environmental, and other factors form a context for establishing one's goal and for defining the means that might or should be successful in reaching it.

The proposed analysis of personal control hypothesizes that P's ability to control successfully private information decreases as the number of recipients increases. It also hypothesizes that the competence to control transmissions and to properly "read" and interpret received messages is not uniform either across senders or for the same sender at different times, under different circumstances, and across types of private information.

The relationship between the concepts of personal control and of privacy are complex. Exercises of control that attain privacy offer us the opportunity to assess and evaluate our personal experiences with these exercises of control. These assessments and evaluations are an important determinant of our judgments of ourselves and of others. Moreoever, our successes and failures at attaining outcomes and objectives are also informative to others; they tell others about ourselves. Insofar as people want to manage the information others have about them, failures can damage an impression. This can be costly. This is a reason why people prepare themselves emotionally and practice their skills in private. Privacy minimizes the chances that information that could damage an impression becomes public. Paradoxically, people need enough competence to successfully obtain privacy in order to have the opportunity to "fail" in the practice or exercise of other behaviors. Moreover, when a "loss of control" also precipitates a loss of privacy -- that is, O gains access to personal information about P above and beyond that which signifies that control was lost -- then P must contend with two sources of costs: those arising from the loss of control and those arising from the loss of privacy. These examples illustrate the complex relationship between the concepts of control and of privacy.

There are settings that permit people only limited control over intimate revelations about themselves. The courtroom is a case in point. In a courtroom, for example during a nasty divorce hearing, personal control is directed at minimizing the potential costs that can arise from revelations. One tactic for P is to recast information about P either by creating a socially acceptable alternative interpretation of events, or by demonstrating that there were mitigating circumstances. Another tactic for P is to blunt the impact of a revelation by O by questioning O's motivation, trustworthiness or credibility. Because the courtoom articulates the thrust and parry of information seeking and information management, it is often used by writers to convey dramatically the portrayal of information management and of personal competence. There also are examples of the exercise of personal control of information that fall beyond the scope of privacy. These include cases in which P controls the flow to O of information over which P has and makes no claim of "ownership" and which is intended for O. This illustrates censorship,

not privacy. Examples such as this demonstrate that information management extends beyond the concept of privacy and that the concept of personal control is a feature of many types of information management, including privacy.

2.5 COSTS

It is assumed that so long as people feel vulnerable and insofar as information about themselves can be a basis for pain or suffering, people will protect that information and will limit access to it to avoid a loss of privacy. Pain and suffering exemplify the social, psychological, or physical costs that motivate privacy behavior. Thus, the privacy of silence or of reserve is an attempt to avoid costs by offering no target for sanctions. However, even silence can be informative and costly, as noted in an example in Section 2.1 of the child who had forbidden treats before mealtime.

The concept of cost is a troublesome one. It has two basic but different meanings (Emerson, 1976). First, there is the psychological meaning of cost as stimulation which one would act to avoid or escape from or reduce. Second, there is the economic meaning of cost as rewards that people forego because resources, such as time or effort, that could have been "invested" in better outcomes or objectives instead were invested in less rewarding outcomes or objectives. Although the first meaning is stressed in this report, both meanings are consistent with how the concept of cost is used in this framework.

With regard to the psychological meaning of cost, costs can vary in their nature, severity, and source. The nature of the costs associated with a loss of privacy include psychological ones -- fear, worry, shame, guilt, remorse -- as well as actual or potential social, material, or physical costs. The severity of reactions to real or imagined or anticipated losses of privacy can vary from mild emotional reactions and simple cognitive reappraisals (Brehm, 1966) to severe, even pathological, reactions including self-destructive acts. The reactions may be culturally appropriate or inappropriate (with suicide a case in point).

At least five hypothesized sources of stress for the person resulting from the loss of privacy have been suggested (although not always in the context of discussions of privacy). These include:

(a) Concern about being stereotyped, or being re-defined by others, in a way that is psychologically damaging; it is a concern about how one will have to present one's self now that the "truth" is out; it is a concern about the attributions that others will make about one's self. In sum, it is a concern about how one is defined by others, and, by implication, about self-definition (Altman, 1975).

(b) Concern about the sheer asymmetry of exposure (you stand naked and exposed while others remain hidden), and about ridicule and contempt by others arising from being found in this situation or from what is revealed (Westin, 1967).

Whereas (a) focuses on how one is defined, (b) focuses on how one is evaluated.

(c) Concern about differential power others gain over one from the loss of privacy. Whether the strategy for control by others stems, for example, from threats (blackmail) or from an increased ability to predict P's behavior, each critically focuses on the behavioral options now open to the exposed person (Johnson, 1975).

(d) Concern about overt punishment (above and beyond ridicule)--imprisonment, exile, torture, death. Punishments also include a loss of privileges, of one's job, of one's money. The loss of friends and the loss of the support of others are also possible forms of punishment.

In (b) the costs are purely psychological; in (d) they are physical, social, and psychological. Speaking metaphorically, (b) represents heaping on you what you do not want, and (d) illustrates taking from you and what you do want.

(e) Concern about self-punitive reactions (e.g, superego reactions, to use the classical psychoanalytic image). P is the target of self-directed negative sanctions: shame, guilt, embarrassment; a feeling of being disgraced, worthless, contemptible. Self-censure is a very potent threat and is one major reason why people limit access to personal information by others. Under special conditions, people even may limit their own access to their "secrets" (e.g., repression).

Cost minimization resulting from privacy behavior has an important positive consequence. There are behavioral options which, because of their form or content, have high cost implications. Without privacy, it is not likely these options would be selected. However, with privacy, the likelihood of these behavioral options being selected increases. For example, the social psychological literature has amply demonstrated that people may not honestly express their "private" opinions if they believe that expressing them "publically" would result in social censure or worse (Berscheid, 1977).

2.6 BOUNDARY REGULATION

Privacy behavior has been described as a boundary regulation process (Altman, 1975). Boundary regulation represents P's understanding, perception and evaluation of conditions whose goal is the successful

separation of P, his/her personal information (X), and perhaps invited recipients and their information, from other, unacceptable potential recipients (O). These conditions include the social relationship between P and O, the nature of the physical setting (see Section 2.7), etc.

Boundary regulation is intimately tied to specific, on-going circumstances including past, present, and future events as currently understood by P. As circumstances change, P may modify his/her privacy behavior in order to maintain control. Persons in conversation who stop talking or suddenly switch topics because a stranger approaches illustrate boundary regulation.

Although the nature of the physical setting directly and powerfully influences the boundary regulation process, boundaries, strictly speaking, are a psychological concept. Nevertheless, the term "boundary" or its synonym "barrier" sometimes will be used metaphorically to suggest a physical shell or membrane that surrounds and/or separates, thereby protecting people and information.

Multiple boundaries are frequent. It is only for analytic convenience that there is a focus on one or another. Moreover, the framework distinguishes between (a) actions that represent, create, or maintain the barrier itself, such as encryption, (b) actions that occur within barriers, typically "private" transmissions, such as self-disclosures, and (c) actions that occur across barriers, such as activities for which anonymity is a precondition.

Two examples, from P's perspective, will illustrate these distinctions. The first example: The conditions that protect conversationalists from uninvited, unacceptable others [Point (a), above] offer the participants an opportunity to share private information among themselves [Point (b), above]. In other words, for P, intimate exchanges [Point (b)] take place within the barrier that separates the participants from uninvited others [Point (a)]. The barrier is a means; the disclosures are its goal (cf. Derlega and Chaiken, 1977).

The second example: Anonymity refers to barriers to personal identification. That is, boundary regulation processes are devoted to protecting indicators of personal identity from being communicated to others. Given anonymity, the probabilities for certain behavioral options increase [Point (c), above]. The options include dealing in questionable or illegal or immoral activities, or trying out or presenting ideas which would otherwise be suppressed. The point is that these activities occur because personal identification is protected. Thus, anonymity is a means for increasing options. The selected option, in turn, can be a means to a desired end.

The concept of boundary regulation focuses on individuals' judgments of their barriers. If two people create similar barriers, the barrier of each remains an individual matter. The idea of two people sharing a single barrier or sharing boundary regulation in any strict sense is rejected. Furthermore, subjective evaluations of barrier effectiveness

need not be accurate nor must the evaluations of barriers by different participants in a given setting be in agreement. Thus, if two person are in a physically isolated setting discussing secret matters, the setting, although physically shared, is not necessarily psychologically shared. That is, each of the individuals can perceive and evaluate the shared setting in ways that might or might not be the same. This example does not mean that the status of the physical environment is limited to its psychological representation. This is not the case, as the next section will forcefully argue.

2.7 THE PHYSICAL ENVIRONMENT

If privacy behavior is P's competence to control the flow and/or content of an information transmission, this competence must be directed at current and future (potential) audiences who might invade or violate P's privacy. Interactions and, by implication, communications with others take place in physical settings. Characteristics of settings influence and shape interpersonal and personal behavior. In turn, an individual can use a physical setting to meet personal or interpersonal ends, for example, by the manipulation of environmental characteristics or by choosing a setting that meets the person's strategic needs. Thus, if we wish to hide the fact that we are in a particular place, we can disguise ourselves, plant a "look out" to monitor intruders, or choose a physical location which permits us to observe others but which does not give others a good opportunity to observe us. A complete theoretical account of interpersonal behavior, particularly of behavior directed at actual and potential audiences, requires an understanding of the physical environment. In sum, the competence to adequately understand and use the environment is a necessary aspect of control over information transmission.

The influence of the built environment on behavior is mediated by the subjective and objective aspects of a setting. The subjective aspects refer to those psychological, social and cultural factors that shape our judgments, perceptions and evaluations of the physical environment. Examples of subjective factors are the influence of culture on visual perception (Segall, Campbell and Herskovits, 1966), social norms about appropriateness of specific settings for specific behaviors (see Wolfe and Laufer, 1975, for examples), and the emphasis on psychological aspects of space, represented by the use of concepts such as territoriality and personal space, in explaining environmental impacts on behaviors (Altman, 1975). Theories that address environmental aspects of privacy tend either to emphasize or more completely explicate these subjective factors (e.g., Altman, 1975).

The objective aspects of the physical environment refer to the enduring, rather than ascribed, characteristics of the physical environment. Objective aspects include the dimensions, shapes and physical properties of objects as well as their distribution and, by implication, organizational in space. These aspects are often mentioned in environmentally-oriented theories of privacy but these aspects are seldom explicated.

A full understanding of objective aspects is still necessary. The objective aspects create the initial conditions or, alternatively, the opportunities for behavior. The subjective factors, by comparison, can influence our evaluation and judgment of the objective aspects, for example, or our selection from among opportunities (cf. Rapoport, 1969). Therefore, without an understanding of the objective aspects, environmental analyses necessarily will remain "one step away" from a complete account of how the spatial characteristics of settings influence the behavior occuring within the settings.

For these reasons, the proposed theoretical analysis of environmental aspects of privacy will focus on the relationship between human sensory capacities and the geography of settings. This theoretical analysis must be able to generate, from physical descriptions of (a) the physical settings, (b) the physical status and personal background of persons in the setting and (c) the location and head-and-body orientation of persons in the setting, estimates of (d) the sensory information--visual, auditory or olfactory--available to the person and (e) the sensory information about the person (arising, for example, from P's appearance, dress, comments, location, posture, etc.) available to others who are or who might enter the settings. The analysis also requires a method for mapping sensory information for all points and head-body orientations in a physical setting. Based on the map, a method is required for determining what information about the environment and others P has or could have access to and the information about P that is or could be exposed to O. We must be able to coordinate this environmental analysis with a behavioral analysis of how P might choose or use his or her position in the setting to personal advantage. Archea (1974, 1977) has developed an environmental analysis that meets many of these objectives. In sum, the proposed theory must provide an objective representation of the physical environment that is behaviorally relevant and must provide the linkages between environmental and behavioral descriptions.

To illustrate what such a theory can be like, Archea's (1974, 1977) access-exposure model of spatial behavior will be described. This is currently the best explanation of spatial behavior which draws on the objective aspects of the environment, provides explicit linkages between environmental and behavioral concepts, and has an associated measurement methodology for mapping the environmental conditions that are visually available to persons in a setting. Moreover, this theory recently has been applied to the concept of privacy (Archea, 1977).[2]

---

[2] The description of Archea's model is from Archea (1977) and all page citations in this section are to this article. However examples and commentary have been added, when appropriate. Only portions of Archea's model are included here. For example, the mapping technique, mentioned above, has been excluded because the early version (Archea, 1974) is under revision; a report on the revised version is in preparation (J. Archea, personal communication, March 1979).

Archea's model builds on the distinction between properties and attributes. Properties are defining characteristics that make things what they are. Properties are always present; they impose limits on what things can do. Attributes are extrinsic characteristics that relate things to other things for specific purposes. Attributes are contingent upon what things do in relation to other things; in effect, they are the performance characteristics of situations created when things come together. Properties, then, are objective characteristics from which all other characteristics of a thing derive their status whereas attributes are conventions. Another important distinction is between settings and situations. Settings are physically and temporally bounded places. Situations consist of activities or events in settings. Thus, settings are environmental whereas situations have both environmental and behavioral characteristics. (p. 119)

For Archea, privacy is an attribute of situations, and not of the environment or of behavior alone. As such, privacy derives its status from constraints that both physical and human properties impose on interpersonal behavior. It follows that a complete understanding of privacy requires a model of spatial behavior that examines settings, social behavior, and their linkages, and which can explain how the objective environment influences social behavior.

Archea's model emphasizes the idea of information fields: "Each person is the center of a dynamic field of information about surrounding events... to which his or her behavior is a continuous adjustment" (p. 121). Thus, the regulation of a person's interpersonal behavior is influenced by the person's possibilities for monitoring information from (the behavior of) others, which Archea calls access, and by the possibilities of others monitoring information about the person's behavior, which is called exposure. That is, a person can have access to information about others and can have their behavior exposed to others. (p. 121)

In this model, visual information is stressed. According to the model, the distribution of visual information is regulated by the physical properties of the environment. Spatial organization, then, establishes the options of those in the setting. Because options can differ in their social consequences for people, spatial organization is critical to what people do and when and where they do it. By properly selecting what, when and where, people can control the impression they create and the social consequences of their behavior for themselves.

Archea advances three derivative propositions. First, situations change over time. Settings, by contrast, are relatively stable over time. Therefore, people have to monitor what is currently happening in a setting and must monitor those places in a setting (such as doors, through which people may suddenly enter a setting) where events could develop. Second, people can manipulate access and exposure be strategically locating themselves in setting. This behavior can control the evaluations and sanctions of others for one's actions in personally desired ways. Third, personal and situational attributes may determine the

effectiveness of visual access and exposure on personal accountability. For example, people may act inappropriately and not be held accountable if they have recognizable excuses for their behavior, such as inexperience or illness. (p. 121)

Expanding on these propositions, behavior is linked to the environment by the manner in which physical properties of the environment, such as the position or opacity of objects, mediate the flow and appearance of information. In turn, people process information in order to coordinate their behavior with both the ongoing and to the anticipated actions of others. Information processing is based on a number of behavioral attributes and their underlying human properties. The behavioral attributes include the person's location and orientation in space, sensory acuity, and familiarity with the setting. The underlying human properties include the structure of memory and the degree of resolution and the directionality of particular sensory equipment. (pp. 122-123) As a result of information processing, people may adjust their behavior. Such adjustments will constitute new information which is distributed across the information field as the organization of the setting permits. Thus, an information field is dynamic.

The influence of the environment is also dynamic. This stems from the ways the environment is used. The principal way is the adjustment of one's position in a setting, or even of the props in a setting (e.g., degree to which a door is open, or the location of a chair or lamp), in order to control what about one's self is exposed to others. This, of course, is the essence of privacy.

With regard to privacy, the model argues that it is easier to selectively conceal and disclose "coextensive" (here-and-now) information than "trace" information. A trace is information which survived, physically or psychologically, the events which initially formed the information. Fingerprints and reputations are examples of trace information. The model also argues that loss of privacy is associated with too much exposure, hence more information is available to others about a person than the person desires. It is also associated with too little access, hence the information needed to gauge the appropriateness of behavior is reduced which increases the probability that the person will present him/herself to others in a way for which the person does do not want to be held accountable. (pp. 129-130).

In sum, Archea's model of spatial behavior links the physical environment with behavioral, particularly social, variables. The role and nature of the physical environment is examined and its applicability to situational attributes, such as privacy, has been explored. Although Archea's 1977 model is not a final statement, it is still a large step toward defining and measuring the physical environment independently of the way in which behavior is typically defined and measured. (p. 134f)

2.8 SUMMARY

As preparation for developing a theory of privacy, a conceptual analysis of privacy was undertaken that provides a framework for theory development. The framework focuses on privacy as strategies of information management that attempt to handle the personally costly consequences of unlimited or unprotected distribution of personal information. The framework stresses social psychological factors. However, it also strongly endorses the view (Archea, 1977; Margulis, 1977a) that a complete understanding of social behavior, including privacy, requires an explicit, account of the nature of the objective physical environment and a clear statement of the relationship between behavior and the physical environment.

3. REFERENCES

Altman, I. Privacy: A Conceptual Analysis. In D. H. Carson (Ed.), Man-Environment Interactions: Evaluations and Applications (Part II, Vol. 6: S. T. Margulis, Vol. Ed.). Stroudsburg, PA: Dowden, Hutchinson and Ross, 1975.

Altman, I. Privacy Regulation: Culturally Universal or Culturally Specific? Journal of Social Issues, 1977, 33(3), 66-84.

Archea, J. Identifying Direct Links Between Behavior and Its Environment: Toward a Predictive Model. In T. O. Byerts (Ed.), Environmental Research and Aging. Washington, D.C.: The Gerontological Society, 1974.

Archea, J. The Place of Architectural Factors in Behavioral Theories of Privacy. Journal of Social Issues, 1977, 33(3), 116-137.

Berscheid, E. Privacy: A Hidden Variable in Experimental Social Psychology. Journal of Social Issues, 1977, 33(3), 85-101.

Brehm, J. Attitudinal Consequences of Commitment to Unpleasant Behavior. Journal of Abnormal and Social Psychology, 1960, 60, 379-383.

Cammock, R. Confidentiality in Health Centers and Group Practices: The Implications For Design. Journal of Architectural Research, 1975, 4(1), 5-17.

Canter, D. and Kenny, C. The Spatial Environment. In D. Canter and P. Stringer, Environmental Interactions: Psychological Approaches to Our Physical Surroundings. London: Surrey University Press, 1975.

Chermayeff, S. and Alexander, C. Community and Privacy. New York: Anchor Books, 1965.

Churchman, A. and Herbert, G. Privacy Aspects in the Dwelling: Design Considerations. Journal of Architectural Research, 1978, 6(3), 19-27.

Convenience Versus Privacy. Building Research and Practice, January/February 1973, 30-31.

Cooper, C. C. Easter Hill Village: Some Social Implications of Design. New York: The Free Press, 1975.

Derlega, V. and Chaiken, A. Privacy and Self-Disclosure in Social Relationships. Journal of Social Issues, 1977, 33(3), 102-115.

Emerson, R. M. Social Exchange Theory. Annual Review of Sociology, 1976, 2, 335-362.

Filipczak, J. A Reflection on Privacy and Programming in Prison. In W. F. E. Preiser (Ed.), Environmental Design Research (Vol. 2, Part 7: E. H. Steinfeld, Symposium Ed.). Stroudsburg, PA: Dowden, Hutchinson and Ross, 1973.

Francescato, G. Weidemann, S., Anderson, J. and Chenoweth, R., Predictors of Residents' Satisfaction in High Rise and Low Rise Housing. Journal of Architectural Research, 1975, 4(3), 4-9.

Goffman, E. The Presentation of Self in Everyday Life. Garden City, New York: Doubleday Anchor Books, 1959.

Johnson, C. A. Privacy as Personal Control. In D. H. Carson (Ed.), Man-Environment Interactions: Evaluations and Applications (Part II, Vol. 6: S. T. Margulis, Vol. Ed.). Stroudsburg, PA: Dowden, Hutchinson and Ross, 1975.

Justa, F. C. and Golan, M. B. Office Design: Is Privacy Still a Problem? Journal of Architectural Research, 1977, 6(2), 5-12.

Kelvin, P. Predictability, Power and Vulnerability in Interpersonal Attraction. In S. Duck (Ed.), Theory and Practice in Interpersonal Attraction. New York: Academic Press, 1977.

Laufer, R. S. and Wolfe, M. Privacy as a Concept and a Social Issue. Journal of Social Issues, 1977, 33(3), 22-42.

Levy, A. S. What Happened to the Environment? (Review of "The Environment and Social Behavior" by I. Altman). Contemporary Psychology, 1976, 21, 615-616.

Margulis, S. T. (Ed.). Privacy. In D. H. Carson (Ed.), Man-Environment Interactions: Evaluations and Applications (Part II, Vol. 6: S. T. Margulis, Vol. Ed.). Stroudsburg, PA: Dowden, Hutchinson and Ross, 1975.

Margulis, S. T. Conceptions of Privacy: Current Status and Next Steps. Journal of Social Issues, 1977, 33(3), 5-21. (a)

Margulis, S. T. Introduction. Journal of Social Issues, 1977, 33(3), 1-4. (b)

Margulis, S. T. (Issue Ed.). Privacy as a Behavioral Phenomenon. Journal of Social Issues, 1973, 33(Whole No. 3). (c)

Mautz, R. K., II. Environmental Manipulation and Extant Conditions. Unpublished manuscript, no date. (Available from the author, 2130 Stone Drive, Ann Arbor, Michigan 48105).

Newcomb, T. M. An Approach to the Study of Communicative Acts. Psychological Review, 1953, 60, 393-404.

Newcomb, T. M. Individual Systems of Orientation. In S. Koch (Ed.), Psychology: A Study of a Science (Vol. 3). New York: McGraw-Hill, 1959.

Prather, J. E., Sociological Observations of Privacy Behavior in a Bank Lobby. Paper presented at the meeting of the American Sociological Association, New Orleans, August 1972.

Rapoport, A. House Form and Culture. Englewood Cliffs, N.J.: Prentice-Hall, 1969.

Sanoff, H. and Sawhney, M., Residential Livability. Raleigh, N.C.: North Carlina State University, 1971. (NTIS No. PB 201 196).

Segall, M. H., Campbell, D. T. and Herskovits, M. J. The Influence of Culture on Visual Perception. Indianapolis: Bobbs-Merrill, 1966.

Thompson, J. D. and Goldin, G. The Hospital: A Social and Architectural History. New Haven: Yale University Press, 1975.

The Trouble With Open Offices. Business Week, August 7, 1978, pp. 84-86.

Veterans Administration. Patient Privacy in VA Health Care Facilities. Washington, D.C.: Department of Medicine and Surgery, Veterans Administration, November 1977.

Warren, C. and Laslett, B. Privacy and Secrecy: A Conceptual Comparison. Journal of Social Issues, 1977, 33(3), 43-51.

Westin, A. Privacy and Freedom. New York: Antheneum, 1967.

What Buyers Say They Want in Housing in 1978. Professional Builder, December 1977, p. 71.

Wilsnack, R. W. Information Control: A Conceptual Framework for Sociological Analysis. Urban Life, in press.

Wolfe, M. and Laufer, R. The Concept of Privacy in Childhood and Adolescence. In D. H. Carson (Ed.), Man-Environment Interactions: Evaluations and Applications (Part II, Vol. 6: S. T. Margulis, Vol. Ed.). Stroudsburg, PA: Dowden, Hutchinson and Ross, 1975.

NBS-114A (REV. 9-78)

U.S. DEPT. OF COMM. BIBLIOGRAPHIC DATA SHEET	1. PUBLICATION OR REPORT NO.	2. Gov't. Accession No.	3. Recipient's Accession No.

4. TITLE AND SUBTITLE

Privacy as Information Management: A Social-Psychological and Environmental Framework

5. Publication Date

6. Performing Organization Code

7. AUTHOR(S)

Stephen T. Margulis

8. Performing Organ. Report No.

9. PERFORMING ORGANIZATION NAME AND ADDRESS

NATIONAL BUREAU OF STANDARDS
DEPARTMENT OF COMMERCE
WASHINGTON, DC 20234

10. Project/Task/Work Unit No.

11. Contract/Grant No.

12. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS *(Street, City, State, ZIP)*

13. Type of Report & Period Covered

14. Sponsoring Agency Code

15. SUPPLEMENTARY NOTES

☐ Document describes a computer program; SF-185, FIPS Software Summary, is attached.

16. ABSTRACT *(A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here.)*

A social-psychological and environmental framework for a theory of privacy is summarized. The framework focuses on the management of information the loss of which would or could have costly consequences for the target of the information. Key concepts, such as information, communication, personal control, cost, and barrier, are defined and discussed. Particular emphasis is placed on influence of the objective physical environment on privacy.

17. KEY WORDS *(six to twelve entries; alphabetical order; capitalize only the first letter of the first key word unless a proper name; separated by semicolons)*

Architectural psychology; bibliography; buildings; communication; cost; human characteristics; personal control; physical environment; privacy.

18. AVAILABILITY ☒ Unlimited

☐ For Official Distribution. Do Not Release to NTIS

☐ Order From Sup. of Doc., U.S. Government Printing Office, Washington, DC 20402, SD Stock No. SN003-003-

☒ Order From National Technical Information Service (NTIS), Springfield, VA. 22161

19. SECURITY CLASS (THIS REPORT)	21. NO. OF PRINTED PAGES
UNCLASSIFIED	27
20. SECURITY CLASS (THIS PAGE)	**22. Price**
UNCLASSIFIED	$4.00

USCOMM-DC