Methodological Obstacles to Empirical Research in Information Privacy

Stacy B. Veeder
School of Information Studies
Syracuse University
sbveeder@mailbox.syr.edu

This paper discusses the methodological difficulties of conducting research in information privacy, an area of information studies that has long been neglected by empiricists in spite of its growing importance. Privacy-related research, by its very nature, introduces special problems for empirical researchers, particularly when they require quantitative data. Very few of the relevant variables have been operationalized, and the literature contains little guidance as to what methodological tools might best elicit meaningful data and facilitate its analysis. And, while non-response bias is a problem in much social-science research, it is of particular concern when studying information privacy because the very object of scholarly interest—attitudes about information privacy, for example—may systematically affect potential respondents' willingness to participate in the research.

Introduction

All social science research raises methodological difficulties. The ability of social scientists to understand the phenomena they study is limited by imprecise and otherwise inadequate measurement tools, and the relevant variables are sometimes difficult to identify, separate, and measure or control. Often, the variables of interest are attributes of an internal state of being (such as a mood, thought, feeling, attitude, or belief) or are in other ways intangible. A number of methodological techniques have emerged to elicit and analyze social science data, but each suffers from some weakness or set of weaknesses, which may be more or less important to the study at hand. Thus, the researcher typically must choose between one technique and another, trade off one drawback for another, weigh the benefits of one approach against the benefits of another.

In the field of information science, these problems are exacerbated when the researcher wishes to explore privacy-related information issues. Advances in information technology over the past several decades have increased organizations' ability to collect, store, use, add value to, and transfer information. These developments, in turn, have given rise to a host of privacy concerns about personal information—specifically, about what information is collected, who collects it, who has access to it, and the purposes for which it is used. Yet little research, other than public opinion polls, exists to help information scientists to understand these concerns and their implications. One reason for this paucity of empirical data on issues related to the privacy of personal information (hereinafter called "information privacy") may be the particular difficulty involved in eliciting relevant and useful data from respondents. Research in the area of information privacy, by its very nature, introduces special problems that are very different from those encountered in studies of relevance, information retrieval, users' information-seeking behaviors, information management, and other traditional areas of information science. While none of these methodological obstacles are unique to the domain of information privacy, they combine in a way that can seriously bias even the most carefully planned privacy-related studies.

This paper begins with a brief look at information privacy and its importance as the object of empirical research. It then reviews the special methodological challenges of researching issues related to information privacy, illustrating why many of the methods of eliciting and analyzing data commonly used in other information science domains are inappropriate for information privacy research. Finally, the paper suggests a methodological alternative that might yield more satisfactory data in this problematical area of inquiry.

Background

Westin (1995, 2) defines information privacy as "the claim of an individual to determine what information about himself or herself should be known to others . . . [including] when such information will be communicated or obtained and what uses will be made of it by others." Other scholars have offered their own definitions (for example, Fried 1968, 210; Mason 1986, 5; National Research Council and Social Science Research Council 1993, 22; Parent 1983, 347; Schoeman 1984; Smith 1994, 1; Stone et al. 1983,. 460; Ware 1993, 195), but nearly all of these definitions share the principle of controlling access to personal information about oneself. Confidentiality, "an obligation not to transmit . . . information to an unauthorized third party" (National Research Council 1991, 289; National Research Council and Social Science Research Council 1993, 22), is a closely related but distinct concept and should be viewed as one means used to protect information privacy. Finally, personal information is "information that most people in a given society at a given time do not want widely known about themselves . . . or facts about which a particular person is extremely sensitive and which he therefore does not choose to reveal about himself . . ." (Parent 1983, 346-347). "Such information is often financial or medical in nature, but does not have to be in order to be personal. It might include an individual's address or phone number, social security number, age or weight, academic grades, military service record, marital status, or a host of other facts that, by themselves might not seem terribly intrusive but together can paint a detailed portrait of the individual" (Veeder 1997, 15).

The notion of information privacy grew out of a changing information environment, one in which disparate facts about an individual's personal life—once stored on paper in far-flung locations, difficult and costly both to locate and to collate, if indeed they had been collected at all—have, through computerization, become easy and relatively inexpensive to find, collate, sort, and sell or share (Privacy Protection Study Commission 1977). Where personal information once may have been aggregated into isolated "data puddles [that] are around for a short while but then dry up and vanish" (Ware 1984, 334), it now resides in large, permanent databanks that contain centrally accessible virtual dossiers on millions of identifiable individuals (Forester and Morrison 1994; Linowes 1989; Regan 1995, 228; Rothfeder 1992; Ware 1993); Flood and Lutz (1997) call these databanks "peoplebases."

More personal information is being collected by more organizations, and its electronic storage, manipulation, and transfer has led to what some researchers call a "digital shadow" (Agre 1994), "digital persona" (Clarke 1994), or "dataprint" (Kilger 1994). Each of these terms is an attempt to label a digital entity that (1) corresponds with a real, identifiable individual and (2) constitutes a multi-dimensional dossier about that individual. Thanks to a new, thriving industry whose stock in trade is the procurement, management, and sale of personal information, this information is no longer used only for the original purpose for which it was collected. More often than not, the worth of personal information is enhanced by the ability to add value to it (Taylor 1986) and/or put it to a host of secondary uses, usually without the data subjects' knowledge or consent (Branscomb 1994, 3-4; Cavoukian and Tapscott 1997; Gellman 1996). Secondary uses are any uses of personal information that are unrelated to the original purpose for which the information was collected. In addition to the creation of targeted mailing lists for use by direct marketers, these uses include such practices as computer matching (Agranoff 1991; Cavoukian and Tapscott 1997; Clarke 1994; Gellman 1996; National Research Council and Social Science Research Council 1993; Ware 1994), computer profiling (Clarke 1994), computer blacklisting (Agranoff 1991), and other forms of what Clarke calls "dataveillance" (data + surveillance), which he defines as the "systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons" (Clarke 1994, 83). Recent surveys indicate that 80 percent of all Americans feel that "consumers have lost all control over the circulation of their personal information by companies" (Louis Harris and Westin 1993, 1995), reflecting the earlier findings of the Privacy Protection Study Commission (1977).

At the same time, Regan (1995) believes that privacy has "instrumental value," in that it serves as a means of achieving other ends (Institute of Medicine 1994, 145), primarily by facilitating the development of trust. For example, the same federal statutes that require all individuals who live or earn income within the United States to provide the Bureau of the Census (Title 13, U.S.C.) and the Internal Revenue Service (Internal Revenue Code, Sections 6001, 6011, 6012(a)) with personal information also require those agencies to keep this information strictly confidential (Title 13, U.S.C.; Internal Revenue Code, Section 6103), a requirement intended to encourage compliance with the mandatory self-disclosure clauses (Linowes 1989, 89; Westin 1967, 50). In like manner, all U.S. citizens are guaranteed the right to cast secret ballots in elections at all levels of government; privacy in the voting booth is intended to increase voter turnout and to encourage voters to vote their consciences without fear of retribution. In health care, hiv testing procedures offer confidentiality protections not available for other sexually transmitted diseases, an artifact from the early days of the aids epidemic, when, in the absence of effective treatment, there was little incentive for potential carriers of the virus to risk the social stigma and discrimination associated with coming forward to be tested and monitored.

Thus, while most public policy debates position privacy as an individual right (Regan 1995), actual policy decisions often rest on the assumption that assurances of privacy and confidentiality encourage certain socially desirable behaviors. Yet that assumption rests more on intuition than on any body of empirical evidence. If the assumption is correct, then the current trends in the collection and use of personal information and in the creation of digital personae may jeopardize those societal goals. Empirical research is needed to identify and assess any effects these trends, and confidentiality itself, may have on behavior. But the task of collecting the necessary data poses methodological challenges, which may explain why so little empirical work has been done in this area thus far.

Obstacles to Data Collection

The information science literature offers little guidance to empirical researchers interested in studying such phenomena as the effects of confidentiality protections and other privacy-related issues. One problem is that, while there exists a plethora of conceptual definitions of privacy, confidentiality, and related terms, few of these terms have ever been operationalized. Similarly, because this area of inquiry differs from more traditional areas of information science, it is unclear which methodological tools would be best suited to eliciting relevant and useful data.

Information scientists have at their disposal a wide variety of data-collection techniques, each with its own strengths and weaknesses. When applied to the study of such phenomena as information privacy, expectations of confidentiality, and the relationship between those expectations and behavior, however, most of these techniques, even when combined into a multimethod approach as described by Brewer and Hunter (1989), fail to overcome two major sources of potential bias. One source is non-response bias (Fowler 1993, 38-53), a common issue in social science research but of special concern in privacy-related studies. The other source of potential bias is a manifestation of Heisenberg's uncertainty principle (Katzer, Cook, and Crouch 1991, 33). These two problems combine with ethical considerations to make direct observation of privacy-related behavior difficult if not impossible.

Lack of Guidance in the Literature

One of the fundamental difficulties in conducting privacy-related research lies in operationalizing the relevant variables (Katz and Hyman 1993, 252). What is privacy? How do we measure it? Although Westin (1967) and a number of other scholars (Marshall 1974; Schoeman 1984) have attempted to identify the dimensions of privacy, they made no effort to operationalize the term. A group of prominent privacy researchers and practitioners concluded at the 1995 National Privacy and Public Policy Symposium that even defining the slippery concept of privacy was a difficult task; finding a valid way to operationalize it is even more challenging. Related concepts, too, defy operationalization. How, for example, should we measure confidentiality?

Researchers in more conventional information science areas can look to the literature and evaluate the utility of previous attempts to operationalize relevant variables. In designing a relevance study, for example, a researcher could choose to reject recall in favor of precision, or to reject both in favor of a measure of usefulness, making the decision based both on the findings of prior studies and on the arguments put forward in the scholarly debate over the best measure of relevance. The point here is that the relevance researcher is not starting from scratch. Information privacy researchers, on the other hand, have little to build on.

Empirical literature typically provides guidance not only in operationalizing variables, but also in making methodological choices about data collection and analysis. For example, researchers interested in users' information-seeking behavior can determine from reading prior studies that, for example, direct observation (Ingwersen 1982; Mintzberg 1980; Wilson 1997; Wilson and Streatfield 1981), critical incident (Erdelez 1995; Saracevic and Kantor 1997a, 1997b), interviewing (Ellis 1989; Kuhlthau 1988; Wilson, Streatfield, and Mullings 1979), think-aloud (Hert 1995, 1996; Michel 1994; Reneker, 1992), and sense-making (Dervin 1983) might each serve as a useful method of obtaining some or all of the desired data. The information science literature provides a body of experience illustrating circumstances in which one of these techniques might work better than another, depending upon the specific research questions and the researcher's epistemological approach. No such body of empirical experience exists in the information science literature in the area of information privacy.

To be sure, there has been some research conducted into information privacy in disciplines other than information science. Citing E.F. Stone and D.L. Stone (1979), D.L. Stone counts more than 2,000 empirical and theoretical works in this area, but says that "[i]n spite of this large number of privacy-related publications . . . there is a paucity of empirical work dealing with the factors that affect individuals' perceptions of invasion of privacy" (D.L. Stone 1986, 371). Many of the studies that do exist focus primarily on how organizations handle personal information (for example, Bennett 1992; Smith 1990, 1993, 1994) or on factors affecting how such information-handling practices are perceived in consumer situations (Culnan 1993) or employment situations (such as Fromkin et al. 1979; Fusilier and Hoyer 1980; Ganster et al. 1979; Hoylman 1976; Rosenbaum 1973), rather than on how these practices might affect the behavior of the individuals who are the subjects of the information. Psychologists have identified several personality and socio-cultural factors that may affect an individual's willingness to disclose personal information (Aloia 1973; Cozby 1973; Pedersen 1987; Pedersen and Frances 1990; Stone 1986; Vidmar and Flaherty 1985), but their findings are inconsistent. They have also explored the relationship between confidentiality expectations and self-disclosure, but only with special populations in mental-health settings (Cutler 1987; Drake 1992; Taube 1987). Generally, these studies do not offer operationalizations or methodological techniques that would lend themselves well to research exploring the impact of information privacy (or its absence) on the behavior of the people who are the subjects of personal information.

Analyses of privacy in general can be found in legal theory and in philosophy, or even in sociology, but they are not particularly helpful because (a) except for some legal analyses, they focus on other aspects of privacy than information, and (b) they generally do not attempt to propose theoretical relationships among constructs, identify indicator variables, or test hypotheses. Similarly, the series of privacy-related opinion polls conducted by Westin and his associates (e.g., Louis Harris and Associates and Westin 1990, 1991, 1992, 1993, 1994, 1995) have been designed more to document trends in the public's privacy-related attitudes than to explore underlying theoretical issues. In short, considering the overwhelming abundance of written material devoted to the subject of privacy, or even to information privacy alone, there is a void in its development as an object of empirical inquiry.

Non-Response Bias

Another difficulty in conducting research into information privacy is the particularly high likelihood of encountering non-response bias. Because ethical considerations require that participation in research involving human subjects be voluntary (Babbie 1995, 447-449), sampling a population in social science research often relies upon a certain degree of respondent self-selection. If respondents randomly participate or fail to participate in a study, there is no bias.

More often than not, however, there is a systematic effect at work; that is, members of the desired sample who choose not to participate in the research may share one or more traits that distinguish them from sample members who do participate. For example, Fowler (1993, 41) suggests that "people who have a particular interest in the subject matter or the research itself are more likely to return mail surveys than those who are less interested." This systematic effect, regardless of its cause, is called non-response bias. As Alreck and Settle (1995, 35) observe, "Nonresponse bias is a very serious problem when there's a direct connection between the purposes of the [research] . . . and likelihood to respond . . . The variable being measured . . . would directly affect the likelihood to respond" (emphasis in original).

Therein lies the problem for research examining relationships between information privacy and behavior. Based on a series of annual surveys dating back to 1979 (e.g., Louis Harris and Associates and Westin 1990, 1991, 1992, 1993, 1994, 1995), Westin (1995, 17) concludes that the American public can be divided into three groups based on their feelings about information privacy:

> Privacy fundamentalists are "very worried about losses of their privacy and what they see as improper commercial and governmental demands for their data; they seek strong legal rules to forbid such data collection and use."
>
> Privacy pragmatists "care about privacy, but also want access to consumer benefits, believe business have a right to get information when they are asked to grant credit, insurance, or employment, and see public-records disclosure and reasonable law enforcement surveillance as social interests also to be met."
>
> The privacy unconcerned are those people "who give their personal information gladly to get commercial opportunities and benefits, support broad law enforcement access to personal data, and simply do not see privacy as a real issue."

Echoing Fowler (1993), Alreck and Settle (1995, 35) write that "those who are highly involved with the [research] topic are more likely to respond than those who aren't" regardless of whether the strong feelings are positive or negative. If this is true, then privacy fundamentalists may be more likely than the privacy unconcerned to participate in privacy-related research; privacy pragmatists' participation may depend on whether they see some clear personal benefit to participating. Alternatively, because respondents might perceive the research itself as an invasion of privacy, privacy fundamentalists might be more likely than the privacy unconcerned to choose not to participate in the research. Either way, a respondent's attitudes about information privacy may well have a "direct connection" to his or her willingness to participate, making non-response bias a major concern.

Ordinarily, data-collection methods that involve personal interaction, such as interviewing, help to mitigate non-response bias (Alreck and Settle 1995, 32-37; Dillman 1978, 51, 53), while mail surveys provide little opportunity for the researcher to overcome a non-respondent's reluctance to participate. As Fowler (1993, 45) says, "Writing a letter is not a very effective way to convince a high percentage of people to do something. Personal contact is significantly more effective than a letter." Alreck and Settle (1995, 36) go even further: "If the interaction [between the variable being measured and the likelihood to respond] is thought to be too strong, the data have to be collected in interviews."

Interviews may work well when the cause of the non-response bias is non-respondents' lack of interest in information privacy issues. But personal interaction may actually increase any non-response bias due to non-respondents' perception that the research in question poses an invasion of privacy. The personal exchange may make respondents more aware that they are sharing personal information with the researcher, who will then use that information for his or her own purposes, regardless of whether those purposes directly benefit the respondents. Privacy fundamentalists and at least some privacy pragmatists may be even more unwilling to reveal anything about themselves to a person than they would have been through an impersonal means, such as a mail survey.

Uncertainty Principle

A second source of potential bias is Heisenberg's uncertainty principle, which states that the very process of observing a phenomenon changes the phenomenon being observed (Hawking 1988; Katzer, Cook, and Crouch 1991, 33). This principle is particularly relevant to research designed to uncover respondents' implicitly held attitudes, beliefs, or expectations (for convenience, referred to hereinafter as a "mindset"). The data-elicitation technique(s) used must be subtle enough to reveal an implicit mindset without causing the respondent to think explicitly about it; if the respondent examines the mindset too closely, he or she may come to the conclusion that it is somehow incorrect or inappropriate and alter it accordingly.

For example, one privacy-related variable is how confidentially respondents think personal information about themselves will be treated by the organizations that collect it. While public opinion polls (for example, Louis Harris and Associates and Westin 1990, 1991, 1992, 1993, 1994, 1995) show that the public is aware that organizations use and circulate personal information, there are many occasions when even privacy fundamentalists might disclose personal information, implicitly expecting that the information will be held confidentially. Suppose that the specific question of interest to the researcher centers on respondents' confidentiality expectations in a health-care setting. Some respondents, without ever consciously thinking about it, might implicitly believe that (1) only the physician and nurse have access to the information in a patient's medical records, and that (2) this information never leaves the physician's office.

If a researcher were to ask such a respondent about this belief (e.g., "Who, if anyone, do you think has access to the information in a patient's medical file?"), however, the respondent may give this implicit belief more thought and come to realize that (a) the insurance company has access to at least some of the information in a patient's record, as might anyone in the physician's office responsible for billing or for referrals; and (b) the physician may share the information with colleagues and/or specialists. As the respondent begins to see these and other possibilities, his or her expectation of confidentiality changes to accommodate them, transforming the initial expectation—the phenomenon the researcher wanted to measure—into a different expectation, one created as a consequence of the researcher's question. Thus, to discover a respondent's implicit expectations without changing them, the researcher must find a way to elicit the data without making the question explicit in the mind of the respondent.

Given this constraint, many techniques traditionally used in information science research may not work well to elicit implicit mindsets. The conversational nature of interviews, for example, makes them especially likely to introduce bias due to the uncertainty principle. Although they may reduce some non-response bias, interviews encourage the respondent to reflect on the researcher's questions. Unstructured interviews may be even more problematic than structured interviews, because the flexibility inherent in unstructured discourse may increase the likelihood that new realizations affecting the mindset will occur to the respondent. Focus groups also exacerbate the risk: One respondent who undergoes the thought process described above can and probably will influence other respondents who might not have otherwise experienced the shift in perspective.

The use of surveys may lessen the risk slightly, but do not eliminate it. Again, by asking respondents to think about their expectations enough to answer the questions, the researcher inadvertently encourages respondents to think about their expectations enough to change them, but careful ordering and wording of the questions can be critical in reducing bias. Close-ended surveys should be avoided, though, because they suggest answers that might not have occurred to respondents, increasing the possibility that their expectations—and responses—will change as a result of reading the survey.

Inability To Observe Privacy-Related Behavior

Naturalistic observation has proved a powerful data-collection tool for some purposes (P.A. Adler and P. Adler 1994), but it is of little help to privacy researchers who might want to correlate respondents' mindsets about information privacy with certain behaviors. For example, if the research question concerns the relationship between how confidential patients believe their medical records to be and how willing they are to provide personal information to a health-care provider, then the researcher ideally would measure the expectations (facing the methodological problems described above) and then observe the patients' behavior with a health-care provider. Unfortunately, such observation usually faces insurmountable obstacles.

The first two obstacles are non-response bias and the uncertainty principle. Many patients would refuse to allow an observer to witness their interactions with a physician. As described above, this refusal is likely to be systematically related to respondents' attitudes about information privacy, as well as to other factors (e.g., body modesty). Even in cases where patients do consent to having an observer present, the interaction between doctor and patient may be affected by the knowledge of the observer's presence (even if that presence is obscured, say, by a one-way mirror). The effect may be apparent in the patient's behavior, the doctor's behavior, or both. Any variance between the observed behavior and the behavior that would have occurred had the observer not been present taints the desired data. Unfortunately, it is impossible to measure that variance.

The third obstacle is that the researcher's presence may violate ethical standards. By raising questions in the actual health-care setting concerning confidentiality, and by imposing himself or herself into the doctor-patient relationship, the researcher may inadvertently interfere with patients' health care in two ways. First, the confidentiality questions may undermine the respondents' trust in their health-care providers. Second, any behavioral changes that occur as a result of the observer's presence (e.g., a respondent who decides, because of embarrassment in front of the observer, not to tell the doctor about certain symptoms) may have a negative impact on the quality of the health care.

Experimentation does not work well, either. One can imagine a controlled experiment wherein the researcher gives two or more groups differing expectations concerning how confidentially their personal information will be treated, then elicits (through surveys, interviews, or whatever) some sort of personal information. But how will the researcher measure how truthful the responses are? Even if the same information has already been collected elsewhere (say, by a health-care provider), the researcher may not have access to it for legal or ethical reasons—reasons that are intended to protect patient privacy. And, even if the researcher could access those records, how can he or she be sure that the records themselves are accurate? Respondents who are less than fully candid during the experiment may also have been less than fully candid with the health-care provider when the medical record was created.

An Alternative Approach

One method that might help to overcome these obstacles is the use of written surveys based on vignettes and administered in person.

Vignettes—short, concrete, fictional scenarios—"often are used to elicit complex social judgments on subjects that are sensitive and are difficult to observe in the field" (Constant, Kiesler, and Sproull 1994, 403). So, for example, the researcher might have respondents read several short scenarios, in each of which a patient consults a physician about some health problem and the physician asks for personal health-related information. Questions following each scenario could ask respondents (a) how sensitive the health problem depicted by the scenario is, (b) how sensitive the requested information is, (c) how necessary the information is for treatment, and (d) whether the patient in the scenario should provide the information. Questions in a later section of the data-collection instrument could elicit respondent's expectations about what happens to the information provided to the physician. These questions could be intermixed with other questions unrelated to confidentiality, to disguise the true goal of the research until after data collection has been completed.

This approach employs several integrated strategies to address the biases discussed earlier. The presence of the researcher should decrease non-response bias to the extent that interpersonal contact can overcome respondents' reluctance to participate. The use of scenarios, and the format of having the respondents assume the role of the patient in each scenario, rather than asking them to describe their own behaviors, should impose some emotional distance between respondents and the situations of interest to the researcher, reducing the perceived risk respondents might associate with answering the questions truthfully. Finally, by asking respondents what the fictional characters should do before asking them about their own mindsets may help to reduce the effect of the uncertainty principle, particularly if a variety of non-privacy related questions are mixed in with the questions that are of primary interest.

This technique, too, suffers some weaknesses, of course. The use of vignettes introduces an artificiality that may not reflect real-life behavior, for example. But it is this same artificiality that may elicit more candid responses than would a more realistic format (Constant, Kiesler, and Sproull 1994). Also, the technique requires physical access to the sample, but how that access is attained will depend upon the population. If, for example, the population were college students, one might visit selected classrooms. If the population were the general population of some geographic region (say, a particular city), the researcher might then go to sample members' homes and simply ring the doorbell. While it is often advisable to notify sample members before the study begins, to tell them that they have been selected for the sample and to solicit their cooperation in advance (Chebat and Picard 1991; Duhan and Wilson 1990; Murphy, Dalenberg, and Daley 1990; Tangmanee 1999), such pre-notification would probably not be wise in this kind of study because it could invite non-response bias. Finally, the structured data-collection instrument limits the richness of the data that the researcher can collect. This limitation is a tradeoff for avoiding an in-depth interview that might change the respondents' mindsets.

Conclusion

This paper has described several obstacles facing information scientists who wish to conduct empirical research into the area of information privacy. These obstacles are not unique to this domain of inquiry, and social scientists working in other domains, both within and outside information science, have developed various data-elicitation techniques to overcome them. But these techniques can fail when applied to privacy-related research. In spite of a public and scholarly interest in information privacy that has been growing steadily for more than 20 years, little empirical research has been conducted in this area thus far.

Because the information science literature offers so little empirical guidance to privacy-related research, there is no evidence that the vignette-based approach described here has yet been tried in that domain. Veeder (1999) will test its suitability for exploring the relationship between respondents' confidentiality expectations and their willingness to disclose personal information to a health-care provider, the research example used in this paper. If the approach is successful, it should transfer easily to information privacy settings other than health care, enabling researchers to explore phenomena related to information privacy more easily.

This study is only a first step, however. Regardless of the results, further efforts will be necessary to develop a body of empirical knowledge that will help researchers understand information privacy and its implications. Without an empirical foundation, there is little basis for building theory in this area, beyond the already voluminous writings that rest merely upon philosophical or legal analysis. Information scientists interested in privacy research can learn much from the related work conducted in other disciplines, but the psychological and organizational emphases found in most of those studies must be replaced by an emphasis on the impact of the collection, use, and transfer of personal information on the subjects of that information.

References

Adler, Patricia A. and Peter Adler. 1994. "Observational techniques." In *Handbook of Qualitative Research* Ed. Norman K. Denzin and Yvonna S. Lincoln. Thousand Oaks, CA: Sage Publications, 377-392.

Agranoff, Michael H. 1991. "Protecting personal privacy in corporate data bases." *Information Strategy: The Executive's Journal* 7(4): 27-32.

Agre, Philip E. 1994. "Understanding the digital individual." *The Information Society* 10(2):73-76.

Aloia, A. 1973. Relationship Between Perceived Privacy Options Self-Esteem, and Internal Control among Aged People Ph.D. diss., California School of Professional Psychology.

Alreck, Pamela L. and Robert B. Settle. 1995. *The Survey Research Handbook*, 2nd. ed. Chicago, IL: Irwin.

Babbie, Earl. 1995. *The Practice of Social Research*, 7th ed. Belmont, CA: Wadsworth Publishing Company.

Bennett, Colin J. 1992. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States.* Ithaca, NY: Cornell University Press.

Branscomb, Anne Wells. 1994. *Who Owns Information? From Privacy to Public Access.* New York, NY: Basic Books.

Brewer, John and Albert Hunter. 1989. *Multimethod Research: A Synthesis of Styles.* Newbury Park, CA: Sage Publications.

Cavoukian, Ann and Don Tapscott. 1997. *Who Knows: Safeguarding Your Privacy in a Networked World.* New York, NY: McGraw-Hill.

Chebat J. and J. Picard. 1991. "Does prenotification increase response rate in mail surveys? A self-perception approach," *Journal of Social Psychology* 131(4): 477-481.

Clarke, Roger. 1994. "The digital persona and its application to data surveillance," *The Information Society* 10(2): 77-92.

Constant, David, Sara Kiesler, and Lee Sproull. 1994. "What's mine is ours, or is it? A study of attitudes about information aharing." *Information Systems Research* 5(4): 400-421.

Cozby, Paul C. 1973. "Self-disclosure: A literature review." *Psychological Bulletin* 79(2): 73-91.

Culnan, Mary J. 1993. "'How did they get my name?': An exploratory investigation of consumer attitudes toward secondary information use." *MIS Quarterly* 17(3): 341-363.

Cutler, Wendy R. 1987. Informed Consent to Limited Confidentiality: Effects on Client Self-Disclosure Ph.D. diss., Southern Illinois University at Carbondale.

Dervin, Brenda. 1983. "An overview of sense-making research: Concepts, methods, and results to date." Paper presented to annual meeting of the International Communication Association, Dallas, Texas (May).

Dillman, Don A. 1978. *Mail and Telephone Surveys: The Total Design Method.* New York, NY: John Wiley & Sons.

Drake, David Warren. 1992. The Effects of Different Confidentiality Conditions on Adolescent Minor Patients' Self-Report of Behavioral and Emotional Problems (Behavioral Problems) Ph.D. diss., North Texas State University.

Duhan, D.F. and R.D. Wilson. 1990. "Prenotification and industrial survey responses." *Industrial Marketing Management* 19(2):95-105.

Ellis, David. 1989. "A behavioural approach to information retrieval system design." *Journal of Documentation* 45(3):171-212.

Erdelez, Sanda. 1995. Information Encountering: An Exploration beyond Information Seeking. Ph.D. diss., Syracuse University.

Flood, Barbara and William E. Lutz. 1997. "Evanescent personal privacy: How we are giving personal privacy away on purpose." In *Information Privacy, Security and Data Integrity: Proceedings of the 1997 ASIS Mid Year Meeting , Silver Spring, MD,* 63-70. American Society for Information Science.

Forester, Tom and Perry Morrison. 1994. *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing,* 2nd ed. Cambridge, MA: MIT Press.

Fowler, Floyd J. Jr. 1993. *Survey Research Methods,* 2nd ed. Newbury Park, CA: Sage Publications.

Fried, Charles. 1968. "Privacy." *Yale Law Journal* 77(3): 475-493.

Fromkin, H.L., J. Adams, D.C. Ganster, M. McCuddy, P.D. Tolchinsky, and R.W. Woodman. 1979. Some Employee Perceptions of Information Practices in Large Organizations: Propriety, Comfort, and Invasion of Privacy, Working Paper 5 Unpublished manuscript: Purdue University, Information Privacy Research Center.

Fusilier, Marcelline R. and Wayne D. Hoyer. 1980. "Variables affecting perceptions of privacy in a personnel selection situation." *Journal of Applied Psychology* 65(5): 623-626.

Ganster, D.C. et al. 1979. "Information privacy in organizations: An examination of employee perceptions and attitudes," *Proceedings of the 39th Annual Conference of the National Academy of Management* 262-266.

Gellman, Robert M. 1996. "Privacy." In *Federal Information Policies in the 1990s: Views and Perspectives,* Ed. Peter Hernon, Charles R. McClure and Harold

C. Relyea. Norwood, NJ: Ablex Publishing Corporation 137-163.

Hawking, Stephen W. 1988. *A Brief History of Time: From the Big Bang to Black Holes..* New York, NY: Bantam Books.

Hert, Carol A. 1995. Exploring a New Model for the Understanding of Information Retrieval Interactions . Ph.D. diss., Syracuse University.

Hert, Carol A. 1996. "User goals on an online public access catalog." *Journal of the American Society for Information Science.* 47(7): 504-518.

Hoylman, F.M. 1976. The Effect of Personal Control and Instrumental Value on the Experience of Invasion of Privacy Ph.D. diss., Purdue University.

Ingwersen, P. 1982. "Search procedures in the library—Analyzed from the cognitive point of view." *Journal of Chemical Education.* 38(3): 165-191.

Institute of Medicine, Committee on Regional Health Data Networks. 1994. *Health Data in the Information Age: Use, Disclosure, and Privacy,* Ed. Molla S. Donaldson, and Kathleen N. Lohr. Washington, DC: National Academy Press.

Katz, James E. and Merton M. Hyman. 1993. "Dimensions of concern over telecommunications privacy in the United States." *The Information Society* 9(3): 251-275.

Katzer, Jeffrey, Kenneth H. Cook, and Wayne W. Crouch. 1991. *Evaluating Information: A Guide for Users of Social Science Research,* 3rd ed. New York, NY: McGraw-Hill Inc..

Kilger, Max. 1994. "The digital individual." *The Information Society* 10(2): 93-99.

Kuhlthau, Carol C. 1988. "Developing a model of the library search process." *Reference Quarterly* 28(2): 232-242.

Linowes, David F. 1989. *Privacy in America: Is Your Private Life in the Public Eye?* Urbana, IL: University of Illinois Press.

Louis Harris and Associates and Alan F. Westin. 1990. *The Equifax Report on Consumers in the Information Age* Atlanta, GA: Equifax Inc.

Louis Harris and Associates and Alan F. Westin. 1991. *Harris-Equifax Consumer Privacy Survey, 1991* Atlanta, GA: Equifax.

Louis Harris and Associates and Alan F. Westin. 1992. *Harris-Equifax Consumer Privacy Survey, 1992* Atlanta, GA: Equifax.

Louis Harris and Associates and Alan F. Westin. 1993. *Harris-Equifax Health Information Privacy Survey, 1993* Atlanta, GA: Equifax.

Louis Harris and Associates. 1994. *Harris-Equifax Health Information Privacy Survey, 1994* (New York, NY: Equifax.

Louis Harris and Associates and Alan F. Westin. 1995. *Harris-Equifax Mid-Decade Consumer Privacy Survey.* Atlanta, GA: Equifax.

Marshall, Nancy J. 1974. "Dimensions of privacy preferences." *Multivariate Behavioral Research* 9: 255-272.

Mason, Richard O. 1986. "Four ethical issues of the information age." *MIS Quarterly* 10(1): 4-12.

Michel, D.A. 1994. "What is used during cognitive processing in information retrieval and library searching? Eleven sources of search information." *Journal of the American Society for Information Science* 45(7): 498-514.

Mintzberg, Henry. 1980. *The Nature of Managerial Work.* Englewood Cliffs, NJ: Prentice Hall.

Murphy, P.R., D. . Dalenberg and J. M. Daley. 1990. "Improving survey responses with postcards." *Industrial Marketing Management* 19(4): 349-356.

National Research Council. 1991. *Computers at Risk: Safe Computing in the Information Age.* Washington, DC: National Academy Press.

National Research Council and Social Science Research Council. 1993. *Private Lives and Public Policies: Confidentiality and Accessibility of Government Statistics*, Ed. George T. Duncan, Thomas B. Jabine, and Virginia A. de Wolf. Washington, DC: National Academy Press.

Parent, W.A. 1983. "Recent work on the concept of privacy." *American Philosophical Quarterly* 20(4): 341-355.

Pedersen, Darhl M. 1987. "Sex differences in privacy preferences." *Perceptual and Motor Skills* 64(3): 1239-1242.

Pedersen, Darhl M. and Frances, S. 1990. "Regional differences in privacy preferences." *Psychological Reports* 66(3, pt. 1): 731-736.

Privacy Protection Study Commission. 1977. *Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission*, Stock No. 052-003-00395-3 Washington, DC: Government Printing Office, July.

Regan, Priscilla M. 1995. *Legislating Privacy: Technology, Social Values, and Public Policy.* Chapel Hill, NC: University of North Carolina Press.

Reneker, Maxine. 1992. Information Seeking Among Members of an Academic Community. Ph.D. diss., Columbia University.

Rosenbaum, B.L. 1973. "Attitude toward invasion of privacy in the personnel selection process and job applicant demographic and personality correlates." *Journal of Applied Psychology.* 58: 333-338.

Rothfeder, Jeffrey. 1992. *Privacy for Sale: How Computerization Has Made Everyone's Private Life an Open Secret.* New York, NY: Simon and Schuster.

Saracevic, Tefko and Paul B. Kantor. 1997a. "Studying the value of library and information services. Part I. Establishing a theoretical framework." *Journal of the American Society for Information Science.* 48(6): 527-542.

Saracevic, Tefko and Paul B. Kantor. 1997b. "Studying the value of library and information services. Part II. Methodology and taxonomy." *Journal of the American Society for Information Science* 48(6): 543-563.

Schoeman, Ferdinand David (ed.). 1984. *Philosophical Dimensions of Privacy: An Anthology* Cambridge, England: Cambridge University Press.

Smith, Henry Jefferson Jr. 1990. *Managing Information: A Study of Personal Information Privacy (Personal Information).* D.B.A. diss., Harvard University.

Smith, H. Jeff. 1993. "Privacy policies and practices." *Communications of the ACM* 36(12): 105-122.

Smith, H. Jeff. 1994. *Managing Privacy: Information Technology and Corporate America.* Chapel Hill, NC: University of North Carolina Press.

Stone, Dianna L. 1986. "Relationship between introversion/extroversion, values regarding control over information, and perceptions of invasion of privacy." *Perceptual and Motor Skills* 62(2): 371-376.

Stone, Eugene F., Hal G. Gueutal, Donald G. Gardner, and Stephen McClure. 1983. "A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations." *Journal of Applied Psychology* 68(3): 459-468.

Stone, Eugene F. and Diana L. Stone. 1979. *Information Privacy: A Bibliography with Key Word and Author Indices*, Working Paper 6 (Unpublished manuscript, Purdue University, Information Privacy Research Center).

Tangmanee, Chatpong. 1999 (anticipated). The Use of Computer-Mediated Communication Systems by Programmers Ph.D. diss., Syracuse University.

Taube, Daniel O. 1987. Effects of Limited Psychotherapeutic Privacy on Patient Disclosure at Intake . Ph.D. diss., Hahnemann University Graduate School.

Taylor, Robert S. 1986. *Value-Added Processes in Information Systems* Norwood, NJ: Ablex Publishing Corporation.

Veeder, Stacy B. 1997. "Problems and issues in information privacy." In *Information Privacy, Security and Data Integrity:: Proceedings of the 1997 ASIS Mid Year Meeting Silver Spring, MD: 15-21.* Ed. Gregory B. Newby. American Society for Information Science.

Veeder, Stacy B. 1999 (anticipated). Confidentiality Expectations and Willingness to Disclose Personal Information to a Health-Care Provider. Ph.D. diss., Syracuse University.

Vidmar, Neil and David H. Flaherty. 1985. "Concern for personal privacy in an electronic age." *Journal of Communication* 35(2): 91-103.

Ware, Willis H. 1984. "Policy aspects of privacy and access." *The Information Society* 2(3/4): 327-350.

Ware, Willis H. 1993. "The new faces of privacy." *The Information Society* 9(3): 195-211.

Ware, Willis H. 1994. *Privacy Dimensions of Medical Record Keeping*, P-7846 Santa Monica, CA: RAND.

Westin, Alan F. 1967. *Privacy and Freedom* New York, NY: Atheneum.

Westin, Alan F. 1995. "Privacy in America: An historical and socio-political analysis." Background paper, National Privacy and Public Policy Symposium, Hartford Connecticut, November 3-4.

Wilson T.D. 1997. "Information behaviour: An interdisciplinary perspective." *Information Processing & Management.* 33(4): 551-572.

Wilson, T.D. and D.R. Streatfield. 1981. "Structured observation in the investigation of information needs." *Social Science Information Studies* 1(3): 173-184.

Wilson, T.D., D. R. Streatfield, and C. Mullings. 1979. "Information needs in local authority social services departments: A second report on Project iniss." *Journal of Documentation* 35(2): 120-136.