"How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use

By: Mary J. Culnan
School of Business
Georgetown University
Washington, D.C. 20057-1008 U.S.A.

Abstract

Strategic uses of information technology based on personal information may raise privacy concerns among consumers if these applications do not reflect a common set of values. This study addresses what differentiates consumers who object to certain uses of personal information from those who do not object. Data collected by questionnaire from young consumers are used to identify a research approach for investigating attitudes toward the secondary use of personal information for direct marketing. Secondary information use occurs when personal information collected for one purpose is subsequently used for a different purpose. While secondary information use is both widespread and legal, it may be viewed as an invasion of privacy when it occurs without the knowledge or consent of the consumer. The setting for the study is the use of point-of-sale data from a supermarket frequent shopper program to generate direct mail solicitations.

Control emerges as a clear theme in differentiating individuals with positive overall attitudes toward secondary information use from those with negative attitudes. Study participants with positive attitudes are less concerned about privacy (measured as control over personal information), perceive shopping by mail as beneficial, and have coping strategies for dealing with unwanted mail. The results also suggest that theory related to categorization of strategic issues as positive-negative with outcomes that are controllable/uncontrollable provides a basis for understanding differences in the ways individuals perceive practices involving personal information. Future research should focus on the specific characteristics of secondary use practices, including the sensitivity of the information, its source, its perceived relevance to the original transaction, and whether disclosure reflects informed consent or results in a potentially harmful outcome to the individual.

Keywords: Privacy, direct marketing, consumer attitudes

ISRL Categories: AI0106, BD0105

Introduction

> I'm not a stamp collector, gourmet cook or bird-watcher, and I don't have children under 18 at home anymore. You're wasting money on me. Where did you get my name . . . and why?
>
> —Joan Harris, "An Open Letter to My Friends in Direct Marketing," *Target Marketing*, May 1990, p. 44.

In April 1990, Lotus Development Corporation proudly announced its plans to release the Lotus MarketPlace: Households. According to the trade press, MarketPlace was expected to revolutionize the mailing list industry by making names, addresses, demographic information, and prior purchase behavior data for 120 million U.S. consumers available on a CD-ROM. The desktop product was a joint venture between Lotus, Equifax, and one of the country's largest credit bureaus. Public opposition to the product began building in the fall after a *Wall Street Journal* article was circulated at several public computer conferences. In response, Equifax and Lotus issued a joint press release on January 23, 1991, stating that they were canceling the project. The statement indicated that the decision resulted from consumer concerns and "the substantial, unexpected additional costs required to fully address consumer privacy issues" (Culnan and Smith, 1992).

The Lotus MarketPlace is a clear example of the risks companies face when they attempt to develop new strategic uses for information technology based on personal information. However, it is not an isolated example of the conflict and uncertainty that corporate America faces as a result of the current resurgence of consumer interest in privacy. In December 1990, the *Wall Street Journal* published a story describing Blockbuster Video's plans to sell mailing lists based on the subject matter of its customers' video rentals (Miller, 1990). In the publicity wake created by the *Wall Street Journal* article, Blockbuster quickly reversed itself and denied that the company planned to sell or rent its lists (Bates, 1991). Also, in May 1992, the New York state attorney general's office announced an agreement with American Express concerning the use of customer lists for direct marketing. American Express agreed to inform its customers that it tracked their buying habits and used the data to compile mailing lists, which it sold to other companies. American Express further agreed to notify card holders of their ability to "opt out" of such lists (Crenshaw, 1992).

The strength and the tenor of public opposition that surfaced in these three examples clearly caught the four companies off-guard. During the height of the controversy over MarketPlace, Lotus still continued to argue, "What's the big deal?" In fact, MarketPlace was only providing a new platform for small businesses to access some of the same mailing lists that Equifax and other direct marketing firms have been selling to larger companies for some time. The sale of video rental lists by category for direct marketing is legal under the Video Privacy Protection Act of 1988. American Express has a long-standing policy of notifying its customers of their right to remove their names from any mailing lists.

This study addresses consumer attitudes toward one aspect of information privacy, the secondary use of personal information, that is, the use of personal information for other purposes subsequent to the original transaction between an individual and an organization when the information was collected. While secondary information use is currently both widespread and legal, these examples illustrate that the practice may be viewed as an invasion of privacy when it occurs without the implied or explicit consent of the individual. This research explores two questions: (1) What differentiates consumers who object to certain secondary uses of personal information from those who hold positive attitudes toward the same practices? and (2) Why is this important? Detailed knowledge about individual preferences is increasingly valuable to decision makers in the competitive global economy. Advances in information technology facilitate the collection and use of this information. However, as the previous examples illustrate, it may be difficult for firms to pursue the opportunities enabled by technology without risking a consumer backlash if the applications do not reflect a common set of values or a shared understanding about privacy. For example, the 1992 Harris-Equifax Consumer Privacy Survey found that while 79 percent of the public believes computers have improved the quality of life in our society, 67 percent believes that the use of computers must be sharply restricted in the future if privacy is to be preserved (Louis Harris and Associates, Inc., 1992).

There has been little attention to the privacy implications of secondary information use in prior IS research outside of the legal and human rights communities, even though privacy concerns are often fueled by information technology. IS researchers and practitioners alike have traditionally addressed issues related to the *primary* use of information, that is, information collected, processed, or used to support sales, customer service, personnel, inventory, purchasing, or other applications in the context of an ongoing relationship established voluntarily between an organization and its customers, employees, or suppliers. Gaining strategic advantage through information technology, in fact, often depends upon effective secondary use of this information by managers within the organization (Applegate and Wishart, 1990; Bruns and McFarlan, 1987; Culnan, 1989; Porter and Millar, 1985). However, the privacy issues associated with the secondary use of information gathered as a result of these relationships have not been addressed explicitly in the literature. Instead, a number of studies have addressed the privacy issues associated with internal company policies for managing personal information (Goldstein, 1975; Linowes, 1989; Smith, forthcoming; Stone, et. al., 1983; Tolchinsky, et. al., 1981; Woodman et. al., 1982). Also, Straub and Collins (1990) discussed the privacy implications of unauthorized access to personal information resulting from a security breach. Privacy has not been recognized as a major risk

to IS management; a recent article on IS threats dealt only with security risks (Loch, et. al., 1992).

While privacy is clearly a strategic issue for organizations, it should be a priority for information systems (IS) management as well (Mason, 1986). As a company's information steward with a broad view of the business, the chief information officer (CIO) should be in the best position to help his or her firm avoid the crises faced by Lotus or Blockbuster described above. Unfortunately, this is often not the case. A recent study of seven firms in the insurance and financial services industries found that IS managers were unwilling to confront other functional managers about potential privacy violations, even when they found such practices to be personally troubling. Rather, they viewed their job as one of implementing the requirements of the other functions in the organization (Smith, forthcoming).

Consumer privacy has also emerged as a major issue for global firms. The European Community has issued a draft directive on data protection that is far stricter than the voluntary protections currently implemented by many American companies. While the majority of industrialized countries have enacted data protection laws, the approaches to data protection vary (Bennett, 1992; Flaherty, 1989). In the United States, privacy laws aim primarily to protect citizens from the government; protecting individuals from abuses by private-sector record-holders has been legislated in a very targeted or sectorial manner (Reidenberg, 1992). This is in direct contrast to the European approach, where omnibus data protection laws have been enacted that provide individuals with a set of rights related to private sector record-keeping practices and provide a basis for the government to protect citizens from abuses in the private sector (Plesser and Cividanes, 1991). As a result, the ability of American firms to continue to trade openly or to establish new business relationships with the European Community may be jeopardized if, in the eyes of the Europeans, U.S. laws do not provide an adequate level of privacy protection (Commission of the European Communities, 1990; Flaherty, 1989).

This study reports the results of an exploratory investigation of consumer attitudes toward secondary information use. It seeks a preliminary understanding of how overall attitudes toward information privacy and direct marketing can differentiate consumers with positive attitudes from consumers with negative attitudes toward the secondary use of personal information for direct marketing. The results of the study are used to assess whether this conceptual approach has promise for designing subsequent research on information privacy. Because is also hoped that the results will inform IS managers about appropriate business policies they can implement voluntarily to address public concerns about specific information practices that may be perceived as a threat to privacy. Because few legal restrictions apply to the gathering and use of personal information in the U.S., privacy is an ethical issue as well as a business strategy issue (Mason, 1986). Research on consumer attitudes toward privacy can help managers distinguish between the ways they *can* and *should* use personal information.

The results of this study should help firms identify information practices that have the potential to raise a red flag in the eyes of the public and also help them understand what steps they can take to address public concerns about secondary use voluntarily, thereby eliminating incentives for Congress or the states to enact legislation. On a more positive note, the current social environment may also provide opportunities for firms to gain advantage by developing and promoting proactive privacy policies. For example, AT&T has used privacy as a theme in its television commercials to counter a competitor's service where subscribers supply names of "friends and family" in order to qualify for a discount.

Background

Concerns about privacy are not new and often emerge when the public perceives a threat from the existence of new information technologies with enhanced capabilities for surveillance, storage, retrieval, and communication of personal information (Clarke, 1988; Gentile and Sviokla, 1990; Mason, 1986; Miller, 1971; Westin, 1967). In their landmark article, "The Right to Privacy," Warren and Brandeis (1890) first articulated the need to secure for the individual "the right to be left alone." They wrote in reaction to the loss of privacy experienced by the nineteenth century equivalent to paparrazi—instantaneous photographs and newspapers—but they also expressed concern that numerous mechanical

devices were threatening to make true the prediction that "what is whispered in the closet shall be proclaimed from the housetops."

The perceived threats posed by new computerized record-keeping systems helped to bring privacy to the public's attention beginning again in the 1960s (Bennett, 1992). In anticipation of some of the challenges to privacy that these systems would bring, two seminal books were published during this period: Alan Westin's (1967) *Privacy and Freedom*, and Arthur Miller's (1971) *The Assault on Privacy*. In addition, two landmark pieces of legislation were enacted during this period. The Fair Credit Reporting Act was enacted in 1970 to provide privacy protection for consumer credit reports. The Privacy Act of 1974 defines citizens' rights and government responsibility for records maintained by the federal government. The Privacy Act also established the Privacy Protection Study Commission (PPSC) to assess the privacy implications associated with the use of computers to process personal information by the private sector for credit reports, banking, insurance, and medical records, and mailing lists (Privacy Protection Study Commission, 1977). A number of Western European countries passed even more extensive data protection legislation during this period (Bennett, 1992).

In the late 1980s, information privacy again became a public issue, fueled by the coming of age of both database marketing and telemarketing. The media have taken notice of caller ID/automatic number identification systems, as well as new applications for point-of-sale (POS) systems. These and other technologies that promote the collection, analysis, and exchange of detailed personal information, and facilitate the compilation of detailed personal profiles, have caused the public once again to focus its attention on privacy (see, for example, Buchwald, 1992; Cohen, 1991; Miller 1991). In the 1992 Harris-Equifax Survey, 76 percent of the public felt that individuals had lost all control over how personal information about them is circulated and used by companies (Louis Harris and Associates, Inc., 1992).

Consumer attitudes about privacy have been addressed in public opinion surveys (Louis Harris and Associates, Inc. and Westin, 1981; Lou Harris and Associates, Inc., 1990; 1991; Katz and Tassone, 1990; Vidmar and Flaherty, 1985) and in a number of disciplines, including law, political science, sociology, and psychology. Depending on the context, privacy exists when an individual can control social interaction and/or unwanted external stimuli, can make autonomous decisions without outside interference, and/or can control the release and subsequent circulation of personal information (Bennett, 1992; Stone and Stone, 1990; Westin, 1967). Invasions of privacy occur when individuals are unable to control their interactions with the social and physical environment (Laufer, et. al., 1976) or when their actions are unknowingly structured (Simitis, 1987; Smith, 1991). This study focuses on information privacy issues related to the collection, storage, use, and transmission of information (Bennett, 1992). Here, privacy is defined as the ability of an individual to control the access others have to personal information (Schoeman, 1984; Westin, 1967). Based on personal experiences, an individual's concern for privacy is likely to vary over the course of his or her lifetime (Louis Harris and Associates, Inc., 1991).

Underlying any definition of information privacy is an implicit understanding that the individual's interests are balanced with those of society at large. Individuals surrender a measure of privacy in exchange for some economic or social benefit, based on the "calculus of behavior," an assessment of their ability to manage any of the consequences of today's choices in the future (Laufer and Wolfe, 1977). Fair information practices define procedural guarantees, similar to fair trade and labor practices, which allow individuals to balance privacy with an organization's need to know (Bennett, 1992). In the United States, the Code of Fair Information Practices was proposed in a 1973 report published by the U.S. Department of Health, Education and Welfare (1973). The Code is based on the following principles: (1) individuals should have the right to know how organizations use personal information and to inspect their records and correct any errors; (2) individuals should have the right to prevent secondary use of personal information if they object to such use; and (3) organizations that collect or use personal information must take reasonable precautions to prevent misuse of the information.

Some of these principles are reflected in existing U.S. privacy laws (Reidenberg, 1992). Similar principles form the basis of European data pro-

tection laws (Bennett, 1992). Within the computing profession, one tenet of the ACM Code of Professional Conduct is the protection of individual privacy. Recently, the ACM Council affirmed its support for fair information practices and urged its observance by all organizations that collect personal information (White, 1991). In his introduction to the 1991 Equifax survey, Alan Westin argued that the key consumer privacy issue in the 1990s will be to define "what fair information practices the pragmatic majority feels to be called for today, and how best to see that these practices are instituted and observed" (Louis Harris and Associates, Inc., 1991, p. 7).

Prior research suggests that, in general, individuals are less likely to perceive information practices as privacy-invasive when (1) information is collected in the context of an existing relationship; (2) they perceive that they have the ability to control future use of the information; (3) the information collected or used is relevant to the transaction; and (4) they believe the information will be used to draw reliable and valid inferences about them (Baker, 1991; Clarke, 1988; Stone and Stone, 1990; Stone, et. al., 1983; Tolchinsky, et. al., 1981; Woodman, et. al., 1982). Some types of information, such as medical and financial information, have been documented as being more sensitive than other types of information (Lou Harris and Associates, Inc., 1990; Stone, et. al., 1983; Woodman, et. al., 1982). Characteristics of secondary information use are summarized in Table 1.

There is, however, no general theory of secondary information use that links the specific attributes or characteristics of an information practice with the perception by a majority of individuals that the practice is either beneficial or privacy-invasive. For example, Westin (1991) used data from the 1990 Equifax survey to compute a "Willingness to Tradeoff" index, which measured an individual's willingness to trade consumer benefits for a relaxation of privacy interests. However, when the index was tested against overall attitudes toward information use related to credit, insurance, employment, and direct marketing, he found that with the exception of the insurance area, public attitudes toward these tradeoffs were not consistent from area to area. This suggests that public perceptions of what constitutes fair information practices varies from sector to sector.

Table 1. Characteristics of Secondary Information Use

Characteristic	Attributes
Information Sensitivity	Type (e.g., financial, medical, demographic); transaction versus profile
Souce of Information	Existing relationship with consumer or acquired from a third party
Consumer's Perception of Relevance to Original Transaction	Relevant or not relevant
Disclosure May Result in Harm to Individual	Errors; valid vs. invalid inferences
Disclosure Reflects Informed Consent	Notice to consumer; ability to withhold consent

This study has adopted a different approach from that used in prior research where privacy typically served as the dependent variable. In these prior studies, differences in attitudes toward information practices and demographic differences were assessed *after* classifying subjects according to their concern for privacy. This approach may be useful in European countries, for example, where omnibus privacy laws regulate the public and private sectors uniformly. However, the approach is inappropriate for informing theory or practice in the U.S. because the U.S. has adopted a highly targeted, sectoral approach to regulating privacy. As a result, fair information practices are often either implemented voluntarily by organizations or not at all (Bennett, 1992; Plesser and Cividanes, 1991; Reidenberg, 1992). Given this regulatory environment, it makes little sense to study attitudes toward privacy apart from a specific context because public attitudes toward practices in a particular industry are likely to vary based on the extent to which people are able to exercise control over secondary information use of personal information. A more promising approach is to use attitudes toward a specific prac-

tice as the dependent variable, particularly if one goal of the research is to inform business practice or public policy, which requires a single-industry perspective. This is the approach adopted here. For example, if significant differences in attitudes toward a practice reflect demographic differences, firms may need to develop different strategies to communicate with different segments of the population.

These concepts will be applied to a specific context: the secondary use of identifiable personal information to generate direct mail. Direct, targeted mail is one communication medium used in direct marketing defined as the use of targeting to deliver a message directly to a selected, identifiable group of customers or prospects (Yeck, 1992). One goal of direct marketing is to generate a measurable response and/or a transaction from an individual. Targeted marketing is ubiquitous; today, virtually every business uses some form of direct marketing, including a number of traditional consumer goods firms such as Procter & Gamble and Pepsico. According to the Direct Marketing Association (DMA), 66 of the *Fortune* 100 and 190 of the *Fortune* 500 in 1990 used direct marketing (Direct Marketing Association, 1992). While important privacy issues are also raised by access to personal information by the government, insurance companies, and credit granters, and by workplace privacy issues such as pre-employment screening or electronic surveillance of employees by their employers, there are likely to be differences in the ways fair information practices are implemented across these settings; therefore, these issues are beyond the scope of this study.

One way that direct mail differs from these other practices is the potential for harm to the individual. While the misuse of personal information by an employer, a lending institution, or an insurance company can result in an individual being denied employment, credit, or other benefits, the use of personal information to send direct mail to an individual rarely results in substantial harm (Sherman, 1992). "What's wrong with a little extra mail? You can always throw it away" is often the industry response to consumer complaints. In 1977, the Privacy Protection Study Commission (PPSC) concluded that the mere receipt of mail solicitations was not a problem. The problem instead was finding out "how they got my name" (Privacy Protection Study Commission, 1977). To reflect this distinction, the secondary use of personal information is conceptualized in this study as having two dimensions: (1) the information processing activity (acquisition, use, or transfer) and (2) the relationship between the consumer and the firm utilizing the information (existing customer or prospect). For existing customers, the firm may make secondary use of the information within the organization, or it may acquire and use external information. Figure 1 represents these practices as a 3×3 grid.

Within the multi-billion dollar direct marketing industry, personal information moves through a complex web. Access to personal information is enabled by the availability of large commercial databases compiled from public records (e.g., motor vehicle records, real estate records, telephone and other directories) or from responses supplied by consumers on warranty cards or surveys. Mail order firms, department stores, publishers, non-profit organizations, and others also rent or exchange their customer lists through mailing list brokers. Consumer credit reports may also be used for targeted marketing as long as the solicitation includes a firm offer of credit.

Organizations seeking information on consumers may tap into this network in two ways. First, organizations can use their own data to profile their existing customers. These profiles are subsequently used by organizations to identify the demographic and psychographic characteristics of *prospective* customers they wish to target and to rent mailing lists reflecting these characteristics. Second, to enable better targeting of their *existing* customers, organizations may have their customer files overlaid with additional personal information by having a list compiler or list broker match the customer file against a third-party marketing database (Burnett, 1988).

One measure of ethical direct marketing is whether a marketer observes fair information practices in its dealings with the public. The Direct Marketing Association has adopted voluntary guidelines, which state that marketers should notify consumers if their names and addresses may be sold as part of a mailing list and should allow individuals to remove their names from these lists. In addition, the Direct Marketing Association operates a mail preference service (MPS) for the entire industry. By signing up for

	Customer (Internal Info.)	Customer (External Info.)	Prospect
Acquire	1. Profile own customers based on existing transaction data.	2. Acquire new information about existing customers from a third party.	3. Acquire information about prospective customers from a third party.
Use	4. Target own customer for new or repeat business.	5. Market-research or cross-market own customers for new business.	6. Target prospective customers for new business.
Transfer	7. Transfer information about own customers within organization.	8. Transfer information about customers to a third party.	9. Transfer information about prospects to other third parties.

Relationship with Consumer

Note: Information transferred or acquired may include demographic information and/or transaction-specific information.

Figure 1. Dimensions of Secondary Information Use

MPS, individuals ask to have their name removed from all national mailing lists. However, use of MPS by direct marketers is also voluntary.

Research Question

The goal of this study is to profile consumers based on their attitudes toward secondary information use. In order to identify variables that can be used to discriminate between groups that are and are not "information-sensitive," the study addresses the following research question: Do individuals with more positive attitudes toward secondary information use differ from those with more negative attitudes based on (1) their attitudes toward direct marketing and (2) their concern for privacy? The results of the study will be used to assess whether this conceptual approach has promise for designing subsequent research on information privacy.

Prior research found that individuals who believe they can exert more control over events, such as the secondary use of personal information, are less likely to perceive that their privacy is being invaded (Fusilier and Hoyer, 1980; Laufer, et. al., 1976; Stone, et. al., 1983; Tolchinsky, et. al., 1981). The more an individual values privacy, the less control he or she perceives to have over personal information (Stone, et. al., 1983). For example, some privacy advocates express fears that the use of targeted lists is a means of manipulating consumers into "buying your products over and over" (Smith, 1991). This suggests that consumers who have positive attitudes toward secondary information use will also have a lower concern for privacy than those consumers who have negative attitudes toward secondary information use.

The 1990 Equifax Survey found that positive attitudes toward the use of personal information for direct marketing resulted from an understanding of the benefits to the consumer, of the type of information being used, and of the ability to control the use of personal information (Louis Harris and Associates, Inc., 1990). For example, the majority of subjects expressed positive attitudes toward the transfer of names and addresses for direct marketing when the benefits were presented and when they were told that no financial information was transferred and that people who did not wish to receive direct mail could have their names removed ("opt out") from mailing lists (Louis Harris and Associates, Inc., 1990). Overall, this suggests that holding positive attitudes toward secondary information use by direct marketers indicates positive attitudes toward the benefits of direct marketing given the existence

of certain ground rules about personal information use. Figure 2 contains the research model for the study.

Method

Data were collected by anonymous written questionnaire from 126 students enrolled in four sections of an upper-division required undergraduate course on information systems. Completion of the questionnaire was voluntary. The four sections were taught by two different professors. The questionnaire was pre-tested in a focus group with MBA students who had completed a core course on information systems and were familiar with privacy issues. After these students completed each section of the questionnaire, they provided oral feedback to the researcher. The survey instrument was modified prior to being administered based on feedback from the focus group.

Demographic data were collected to determine whether the participants had prior experience as consumers that would cause them to form attitudes about direct marketing, and these are shown in Table 2. Potential exposure to direct marketing solicitations was measured indirectly by asking the participants to report frequencies for actions that would result in their names being placed on mailing lists, such as shopping by mail or phone, using a credit card as opposed to cash for making payments, or contributing to

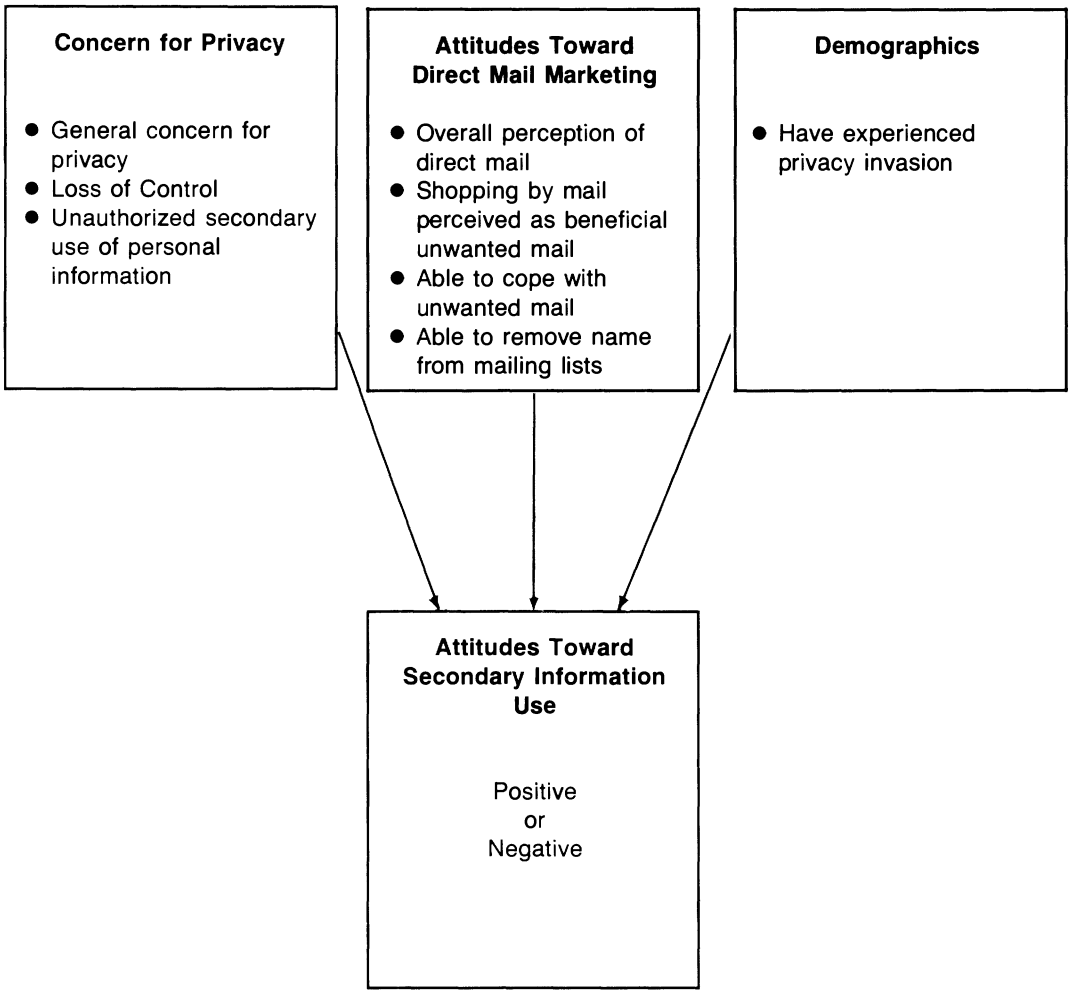

Figure 2. Research Model

a cause. The participants were asked to report the number of times they used their credit card in a typical month, the number of times during the past year they or a member of their household ordered anything by mail, from a catalog, or by calling an 800-number, and the number of times they contributed by mail or phone to a cause they supported. Credit card use was multiplied by 12 to reflect an annual measure of use. The three measures were summed to provide an overall measure of actions/year.

The majority of participants are consumers who have engaged in activities that will result in their names being placed on mailing lists and in the formation of attitudes about secondary information use. For example, a number of students volunteered comments that reflect negative experiences with telemarketing solicitations and receiving mail solicitations for credit cards. All but 11 of the participants (9 percent) have at least one credit card. Eighty-one of the students or a member of their households (64 percent) had ordered something by mail, from a catalog, or by calling an 800-number during the previous year (compared with 48 percent of all respondents for the 1991 Equifax survey). Ninety-three students (74 percent) subscribe to at least one magazine, and 39 students (31 percent) usually return the warranty card when they purchase a product. All but two of the students (2 percent) have engaged in at least one of these activities.

Concern for privacy related to secondary use of personal information, the first independent variable, was measured using five items. In the questionnaire, "personal information" was defined as "any information such as age or income, which is always associated with you as an individual." All items were measured using a five-point ascending Likert-type scale. Table 3 includes descriptive statistics and the wording for all items. Items 1 and 2 were taken from the Equifax surveys (Louis Harris and Associates, Inc., 1990; 1991). Item 3 was taken from a series of earlier Harris polls (Katz and Tassone, 1990). Items 4 and 5 were adapted from a "concern for privacy" instrument developed by Smith, et al. (1992). The psychometric properties for these items have not been established. The five items were factor analyzed using a varimax rotation. Four items load unambiguously on two factors, and these results are also shown in Table 3. The first item, which reflects a general concern for privacy, loaded on both factors. The items on each of the respective factors were summed to form two scales. Factor one represents concern about "loss of control" (Cronbach alpha = .67; $r = .51$, $p < .001$); factor two represents concerns about "unauthorized secondary use" (Cronbach alpha = .69; $r = .52$, $p < .001$).

Because a person's life experiences shape his or her attitudes toward privacy, concern for privacy was also measured using one

Table 2. Demographics

Variable	Yes	No/None	Mean	S.D.
Have Credit Card	114 (90%)	11 (9%)		
Subscribe to at least one magazine	93 (74%)	32 (25%)		
Usually return warranty card for products	39 (31%)	85 (67%)		
Charge/Month		7 (6%)	5.44	4.50
Shop by Mail or Phone/Year		19 (15%)	7.76	20.13
Contributions/Year		82 (65%)	0.77	1.60
Total Transactions/Year		1 (0.8%)	73.88	62.04
Experienced Privacy Invasion?	27 (21%)	89 (71%)		

Note: N = 126. Responses do not add up to 126 due to missing values.

demographic variable, whether a participant believed his or her privacy had been previously invaded (Louis Harris and Associates, Inc., 1991). Twenty-seven students (21 percent) reported that they had personally had their privacy invaded by a company (compared with 23 percent for the same age group in the 1991 Equifax survey).

Attitudes toward direct mail marketing (MAIL), the second independent variable, were measured in two ways. First, overall attitudes toward direct mail were measured by one item from the 1991 Equifax survey by asking the participants whether, overall, they viewed the receipt of catalogs and mail offers at home as "primarily as useful," "rarely use but no problem," "more as a nuisance," or "more as a privacy invasion." The majority of participants hold positive overall attitudes toward direct mail; 72 percent view the receipt of mail offers at home as useful or no problem, while only 2 percent of the subjects view these mail offers as a privacy invasion. This is consistent with the results of the Equifax survey, which found that adults under 30 are the most enthusiastic about the advantages of consumer-based information services and are more willing to engage in tradeoffs involving consumer information uses than other segments of the population (Louis Harris and Associates, Inc., 1990; 1991). In the 1991 Equifax survey, 59 percent of the subjects for the same age group held positive attitudes toward the receipt of direct mail, while 5 percent viewed the receipt of mail offers as an invasion of privacy. For the 1991 Equifax survey, 44 percent of *all* subjects had positive attitudes toward the receipt of direct mail. This variable was recoded as a dichotomous variable; responses of "useful" and "no problem" were combined to form a positive group, while responses of "nuisance" and "invasion of privacy" were combined to form a negative group.

Second, attitudes reflecting benefits/control were measured using seven items developed by the researcher. The items were designed to reflect perceptions about the benefits of direct mail compared with shopping for the same items in a store, and whether the individual perceives that he or she is able to cope with the receipt of unwanted mail (Dutton and Jackson, 1987; Jackson and

Table 3. Descriptive Statistics for Privacy Variables

Questionnaire Item	Mean	S.D.	Inter-Item Correlation 1	2	3	4	Factor Analysis (Varimax rotation) Loss of Control	Unauthorized Secondary Use
1. I am concerned about threats to my personal privacy	3.41	1.04					.66	.37
2. Consumers have lost all control over how personal information is used	3.88	0.97	.46***				.84	.06
3. Americans begin surrendering their privacy the day they open their first charge account	3.81	1.09	.33***	.51***			.81	−.08
4. Companies should not use personal information for any purpose other than the one authorized	4.45	0.79	.26**	.17*	−.01		.05	.87
5. A company should not share personal information about me without my permission	4.45	0.79	.25**	.08	.12	.52***	.07	.85
Eigenvalue							2.07	1.36
% of Variance							41.5%	27.3%

*p≤.05; **p≤.01; ***p≤.001.

Dutton, 1988; Louis Harris and Associates, Inc., 1990). The wording of these items was based in part on the follow-up questions on direct marketing from the 1990 Equifax survey (Louis Harris and Associates, Inc., 1990). All items were measured using a five-point ascending Likert-type scale. Table 4 contains descriptive statistics and wording for all items. The seven items were factor analyzed using a varimax rotation. All items loaded unambiguously on three factors, and these results are also shown in Table 4. The items on each of the factors were summed to form three scales, respectively. Factor 1 represents the benefits of shopping by mail (Cronbach alpha = .54), while factors 2 and 3 represent different coping strategies. Factor 2 represents the ability to cope with unwanted mail (Cronbach alpha = .73); factor 3 represents the ability of individuals to "opt out"—to have their names removed from mailing lists (Cronbach alpha = .42; r = .26, p < .01). Table 5 contains scale means and inter-item correlations for the two privacy sub-scales and the three direct marketing sub-scales.

Mean differences were computed for independent variables in Table 5 based on whether or not the study participant had suffered an invasion of privacy. Only one of the tests yielded a significant difference between the two groups. For one privacy sub-scale, loss of control, the group that reported its privacy had been invaded scored significantly higher than the group that had not experienced a privacy invasion.

Table 4. Descriptive Statistics for Marketing Variables

			Inter-Item Correlation						Factor Analysis (Varimax rotation)		
Questionnaire Item	Mean	S.D.	1	2	3	4	5	6	Benefits of Mail	Cope with Mail	Opt Out
1. Shopping at home saves time over shopping in a store	3.41	1.04							.70	.13	−.12
2. I enjoy being able to shop by mail or phone when it's convenient for me	2.90	1.20	.46***						.89	.03	.08
3. I would be annoyed if I could not receive mail offers or catalogs geared to my interests	2.96	1.23	.03	.32***					.55	.06	−.03
4. It's not a problem to receive catalogs that don't interest me; I just throw them away	3.24	1.32	.16*	.11	.10				.04	.90	−.06
5. It annoys me that I receive so many unsolicited catalogs and mail offers that don't interest me (Reverse-coded)	2.90	1.20	.19*	.18*	.16*	.58***			.18	.86	.09
6. If I choose, I can have my name removed from mailing lists	2.98	1.36	−.05	.03	−.04	.05	.10		.00	.11	.79
7. When I receive mail offers I don't want, I am aware of procedures that allow me to remove my name from these mailing lists	1.83	1.05	−.11	−.03	−.09	−.07	.01	.26**	−.08	−.09	.79
Eigenvalue									1.94	1.34	1.20
% of Variance									27.8%	19.2%	17.1%

*p ≤ .05; **p ≤ .01; ***p ≤ .001.

Table 5. Scale Means and Inter-Item Correlations for Independent Variables

Variable	Number of Items	Scale Mean	Scale S.D.	1	2	3	4	5
1. Overall Concern for Privacy	1	n.a.	n.a.					
2. Privacy-Control	2	7.69	1.71	.44***				
3. Privacy-Unauthorized Secondary Use	2	8.99	1.38	.30***	.08			
4. Benefits of Main Shopping	3	9.27	2.50	−.07	−.05	−.12		
5. Cope with Unwanted Mail	2	6.13	2.24	−.15*	−.22**	−.26**	.21*	
6. Opt Out of Mailing Lists	2	4.81	1.92	.03	.04	−.06	−.06	.02

*$p \leq .05$; **$p \leq .01$; ***$p \leq .001$.

The subjects were also asked two questions based on an item from the 1990 Equifax survey: (1) how much they had heard or read during the past year about the use and potential misuse of computerized information about consumers and (2) *apart from the class*, how much they had heard or read during the past year. Both items were measured using a five-point descending Likert-type scale ranging from "a great deal" to "nothing at all." For the first item, the mean was 2.45 (s.d. = 1.00); for the second item, the mean was 3.05 (s.d. = 1.08). The mean of the difference of the first item minus the second item is −0.60 (s.d. = .80).

Finally, the participants were asked to respond to two open-ended questions. The first question asked for an example of a real or hypothetical situation involving personal information that they believe violates their privacy. The second question asked the participant to list types of personal information that "one company should never share with another company unless you have given them your written permission." Seventy-one responses (56 percent) were volunteered for the first question, and 93 responses (74 percent) were volunteered for the second question. To see if the distribution of responses reflected the participants' prior experiences, whether or not an individual supplied a response to either of the two open-ended questions was cross-tabulated by whether or not the participant had experienced an invasion of privacy. For the first question, where the participants supplied an example of a privacy invasion, there was a significant difference between the two distributions. For participants who had *not* experienced an invasion of privacy, approximately half did *not* volunteer a response to the first question, compared with only one out of seven of the participants who reported that their privacy had been invaded. For the second question, involving the transfer of personal information between organizations, there was no significant difference in the two response distributions.

A grocery store "frequent shopper" program was used as the setting to measure the dependent variable, attitudes toward secondary information use. In these programs, participating individuals voluntarily surrender a measure of their privacy by allowing the grocery store to track their purchases and make secondary use of this information in exchange for receiving some benefit, such as rebates, discounts, or coupons. These programs are typically used to reward participants at the checkout or through the mail for being loyal customers. The programs may also be used to forge strategic alliances with suppliers (Ives, 1989).

The study participants were asked to assume they had joined such a club and would receive coupons and other mail offers in exchange for allowing their purchases to be recorded at the checkout and for allowing the store to know what products each member of the club has pur-

chased. The participants were also given the disclosure statement from a frequent shopper membership application, which read as follows: "I understand and agree that the store may record, make use of, and disclose to other persons or entities any and all of the information I furnish on this application form and information about the products I purchase as a member of this savings club." Given that the majority of participants hold positive attitudes toward direct mail, it was expected that a majority would also feel positively about participating in a frequent shopper program.

All of the study participants had some familiarity with grocery store frequent shopper clubs. At the time of data collection, a major grocery store chain was rolling out its frequent shopper program in the metropolitan Washington area. The rollout was accompanied by a television advertising campaign and an aggressive in-store recruitment campaign at a store within walking distance of the campus. Students in two of the sections had completed a case analysis of a grocery store frequent shopper club (Ives, 1989), while in the other two sections there had been a class discussion of the use of grocery store point-of-sale (POS) data to support decision making. Both professors had also discussed information privacy issues in class. Mean differences were computed for the two groups for the independent variables; none of these differences was significant.

Attitudes toward secondary use, the dependent variable, were measured by 11 items developed by the researcher (POS1 to POS11). Nine of the 11 POS items were developed from the promotional materials for the Citicorp POS database. In addition to using the database to target households that purchase a particular brand-name product or magazine, consumers in the database are profiled as pet owners, weight-conscious, families with children, home bakers, health-conscious, photography enthusiasts, cosmetic buyers, houseware/cookware buyers, fancy food buyers, and coupon clippers based on their purchases. According to the promotional materials, recommended uses of the database include catalogs, general merchandise, high-ticket gifts, books, book clubs and magazines, sweepstakes, or various causes, depending on the individual's prior purchases. The mailing list catalog for a large database compiler and a bank's advertisement for its credit card customer mailing list from a trade publication were used to design the remaining items. A representative item is, "You regularly buy Diet Coke. You receive coupons in the mail from Pepsi-Cola for Diet Pepsi. How do you view this use of personal information?" For all the POS items, the participants were asked to assume they actually purchased the products in the question. All 11 items were measured on a four-point scale by asking the participants to indicate for each item whether they viewed this use of personal information to be (1) primarily useful, (2) rarely useful but no problem, (3) a nuisance, or (4) an invasion of privacy (Louis Harris and Associates, Inc., 1991).

The higher the score for a particular practice, the more negative the respondent's attitude toward that practice. The portion of the questionnaire containing the 11 POS items is contained in the Appendix. Table 6a contains a brief description of each item and the response frequencies for the eleven POS items plus the item about general attitudes toward direct mail marketing (MAIL), the independent variable described above and measured using the same scale. To see if the survey responses reflected differences in the course sections for the subjects, the participants were divided into two groups based on their professor. The responses for the 12 items were cross-tabulated for the two groups. None of the results was significant.

The 11 POS items were designed to represent different characteristics of secondary information use from Table 1 and Figure 1. The disclosure characteristic was not varied because most POS programs do not allow the participants to selectively "opt out" of particular solicitations. While the remaining characteristics were varied across the 11 items, the exploratory nature of the research does not reflect a rigorous experimental design. The secondary use characteristics reflected by the 11 items as defined by the researcher are summarized in Table 6b. Here, "perceived relevance to the original transaction" was defined as solicitations for subsequent purchases at the grocery store or solicitations for a previously purchased item involving another distribution channel, such as a mail subscription for a publication purchased at the grocery store. Only one item, providing a list of names and addresses to an employer (POS6), reflected a "harmful outcome" because disclosing this in-

Table 6a. Response Frequencies for Secondary Information Use Variables

Questionnaire Items (MAIL, POS1 to POS11)	Primarily as Useful	Rarely Use, But No Problem	More as a Nuisance	More as a Privacy Invasion
Overall view of catalogs and mail offers received at home (MAIL)	17 (13%)	75 (60%)	31 (25%)	2 (2%)
POS1. Receive coupons for previously purchased items	97 (77%)	19 (15%)	4 (3%)	5 (4%)
POS2. Receive coupons for a competitive product	38 (30%)	52 (41%)	31 (25%)	4 (3%)
POS3. Receive subscription offer for a magazine previously purchased	77 (61%)	25 (20%)	15 (12%)	8 (6%)
POS4. Environmental group solicits people who buy natural foods and are profiled as "health-conscious"	18 (14%)	43 (34%)	46 (37%)	18 (14%)
POS5. Weight Watchers solicits people who buy low calorie foods and are profiled as "weight-conscious"	12 (10%)	41 (33%)	40 (32%)	32 (25%)
POS 6. Employer mails letter warning of risks of alcohol to employees who buy beer or wine from the grocery store	0	9 (7%)	11 (9%)	105 (83%)
POS7. Dating service solicits people who buy "single serving" products	3 (2%)	19 (15%)	37 (29%)	66 (52%)
POS8. Grocery store overlays database with purchasing power and estimated income data from credit card company	4 (3%)	20 (16%)	20 (16%)	80 (63%)
POS9. Store categorizes customers baed on credit card data and targets people based on their income	29 (23%)	13 (10%)	16 (13%)	66 (52%)
POS10. Grocery store overlays database with motor vehicle, direct mail response, and presence of credit card data from commercial database compiler	9 (7%)	27 (21%)	11 (9%)	76 (60%)
POS11. Book club solicits people who shop by mail, drive a foreign car, and buy paperback books and gourmet foods.	15 (12%)	41 (33%)	38 (30%)	27 (21%)

Note: N = 126. Responses do not add up to 126 due to missing values.

formation could potentially have negative consequences for the employees if the employer chose to single out employees based on the POS data. All of these practices are legal; however, it is unlikely that an ethical marketer would provide a list of people purchasing alcohol to an employer (POS6). The 11 POS items were summed to provide an overall measure of attitudes toward the POS practices (mean = 29.4, s.d. = 5.79, Cronbach alpha = .81). It should be noted that a higher mean score denotes more negative attitudes overall.

Participants were split into two groups based on their scores on the summed POS measure. Participants whose score fell above the mean were classified as being more sensitive to secondary use, while participants whose score fell below the mean were classified as being less sensitive to secondary use.

Table 6b. Secondary Information Use Characteristics for POS Survey Items

Secondary Use Characteristic	Survey Items
1. Type of Information	
• Financial	POS8, POS9
• Transaction	POS1, POS2, POS3, POS6
• Profile	POS4, POS5, POS7, POS10, POS11
2. Source of Information	
• Third Party	POS8, POS9, POS10, POS11
• Existing Customer	All other items
3. Secondary Use Directly Relevant to Original Transaction	
• Yes	POS1, POS2, POS3, POS9
• No	POS4, POS5, POS6, POS7, POS11
4. Potentially Harmful Outcome	
• Yes	POS6
• No	All other items

Results

A discriminant analysis was used to determine if, based on their sensitivity to secondary information use, statistically significant differences exist between the two groups, as well as which independent variables account most for these differences. Here, the analysis measured the effects of the privacy variables (overall concern, control, unauthorized use), the direct marketing variables (overall attitude toward mail, benefits of mail shopping, cope with mail, opt out), and one demographic variable (suffered previous privacy invasion) on each participant's attitudes toward secondary information use, based on whether the subject scored above or below the mean on the summed measure of POS attitudes.

The results of the discriminant analysis are shown in Table 7. Based on the Wilks' lambda of .67 (chi-square = 17.43, $p < .05$), the overall model is significant. Statistically significant differences exist between the two groups. To validate the model, a holdout sample consisting of 50 percent of the observations selected at random was created prior to running the discriminant analysis. The observations in the holdout sample were subsequently classified using the discriminant scores. The discriminant function correctly classified 68 percent of the cases in the holdout sample, which exceeds the "hit rate" that would be expected due to chance (Hair, et al., 1987).

Table 7 also includes the coefficients for the independent variables from the analysis. The probabilities for the F-statistics and the structure matrix coefficients indicate which of the independent variables account for most of the differences between the two groups. The same criteria are used for interpreting the discriminant loadings in the structure matrix as are used for interpreting the results of a factor analysis (Hair, et. al., 1987). Three of the variables are significant and therefore account for most of the differences: privacy measured as control, perceived benefits of shopping by mail, and ability to cope with unwanted mail. The remaining variables (overall concern for privacy, privacy measured as unauthorized secondary use, overall attitude toward direct mail, ability to "opt out," and having experienced an invasion of privacy) are not significant.

Finally, the researcher tabulated the responses to the two open-ended questions. For both questions, many of the participants provided more than one response. The first question asked the participants to cite an example of a privacy invasion involving personal information. The responses included (1) transfer of information across organizations, especially financial, medical or lifestyle information (31 percent of responses); (2) drawing harmful or inappropriate inferences about an individual (14 percent); (3) collecting excessive or irrelevant information (11 percent); (4) an organization being able to "know

Table 7. Discriminators of Attitudes Toward Secondary Information Use

Discriminant Function	
Eigenvalue	0.4861
Canonical Correlation	0.5719
Wilks' Lambda	0.6729
Chi-Squared (df)	17.43 (8 df)
Chi-Squared Significance	.0259
Original Sample Correctly Classified	78%
Holdout Sample Correctly Classified	68%

Discriminant Function Coefficients			
Independent Variable	**Univariate F-Test Probability**	**Standardized Canonical Coefficients**	**Structure Matrix: Pooled Within-Groups Correlations**
Privacy			
Overall Concern for Privacy	.1058	.07	.34
Control	.0173	.66	.51
Unauthorized Use	.2069	.40	.26
Direct Mail			
View Direct Mail Overall	.0725	.28	−.38
Benefits Mail Shopping	.0051	−.58	−.61
Cope with Unwanted Mail	.0121	−.48	−.54
Opt Out	.7943	−.34	−.05
Demographics			
Experienced Privacy Invasion	.7858	.15	.06

about you" as an individual (10 percent); and (5) compiling profiles on individuals (7 percent). Fourteen percent of the responses included general complaints about telemarketing (7 percent) or direct marketing (7 percent).

The second open-ended question asked the participants if there are types of personal information that should never be shared with another company without written permission. The responses included (1) financial information (71 percent of responses); (2) information on lifestyle or "vices" (23 percent); (3) demographic information, including race or marital status (18 percent); (4) medical information (17 percent); and (5) information on an individual's buying practices (8 percent). Twelve percent of the responses stated that *no* personal information should be shared without permission, while 4 percent felt *any* information could be shared without permission.

Discussion and Conclusions

Control emerges from the results of this exploratory study as a clear theme, suggesting that people who are less sensitive about secondary use of personal information have more positive attitudes toward shopping by mail, have developed better coping strategies for dealing with unwanted mail, and have a lower concern for privacy measured as loss of control than people who are more sensitive about secondary use of personal information. One goal of this study was to identify a research approach for investigating how consumers differ in their perceptions about secondary information use. The

relatively homogeneous nature of the sample (young, well-educated, affluent consumers) and the single context of the study (direct mail) limits the external validity of the findings. However, the results are consistent with theory and suggest the approach adopted here is appropriate for future research with a more representative sample (Culnan, 1993).

The results suggest that prior research on how decision makers perceive strategic issues can provide the basis for developing theory on the general characteristics of secondary information use that cause a given individual to perceive a particular practice negatively. Dutton and Jackson (1987) used categorization theory to understand how managers perceive strategic issues. This theory asserts that people form cognitive categories based on their observations of the attributes or features of objects or issues. Categories reflect the structure of objects in the environment and are comprised of objects with similar perceived attributes; they are useful in communication because the information summarized by a category name or label is shared by members of a community. Dutton and Jackson identified two salient strategic issue categories from the strategic management literature—"threat" and "opportunity." Drawing on other literature—from managerial decision making, organizational crises, and individual stress—they hypothesized that three attribute dimensions applied to strategic issues: gain-loss, positive-negative, and controllable-uncontrollable. They found empirical support for their hypotheses in a subsequent study (Jackson and Dutton, 1988).

The results of this study first suggest that categorization theory offers a promising approach for framing future research on secondary information use. Such an approach would investigate how various practices are perceived in terms of the three attribute dimensions identified by Dutton and Jackson (1987). The results of this study also suggest that positive attitudes toward secondary information use for direct marketing reflect a positive view of shopping by mail, including an ability to cope with unwanted mail, as well as a positive attitude toward the use of personal information and the accompanying loss of privacy that is necessary to generate mail solicitations. Additionally, categorization theory has promise for understanding negative attitudes, which reflect a concern for privacy, with control as a core dimension underlying attitudes toward privacy. Finally, because individuals do not perceive all secondary uses of information uniformly, categorization theory also has promise as an approach for understanding differences in the ways individuals perceive particular practices.

Second, the "opt out" variable was not useful in discriminating between high and low levels of information sensitivity. This may be due to the inadequate psychometric properties of the scale used here. It may also be that an awareness of name removal options, in fact, serves both groups equally but in different ways. If fair information practices apply, it should be easy for anyone to have their names removed from mailing lists when they receive unwanted mail. For individuals with low sensitivity to secondary information use, "opting out" serves as a another coping strategy for dealing with unwanted mail. For the other group, opting out may provide a basis for individuals with high information sensitivity to perceive that they can exercise greater control over secondary information use.

Other evidence suggests that these results may be due to low overall awareness of name removal options and that firms need to do a better job of publicizing available options. The 1991 Equifax survey found that 52 percent of the total public was *unaware* of procedures that allow an individual to remove his or her name from direct mail lists. Of those respondents who shopped by mail during the past year, 45 percent were unaware of name removal options (Culnan, 1993). In this study, 78 percent of the participants disagreed with the statement that when they receive mail offers they don't want, they are aware of procedures that allow them to remove their names from these mailing lists. One participant commented, "...I'm not sure what information was bought or sold that prompted tons of junk mail and idiotic phone calls." Another said, "I would like to find out how I can get my name off of certain mailing lists." Still another volunteered, "They say you can [have your name removed from a mailing list], but you *always* end back on it."

There is also reason to believe that direct marketers need to do a better job of implementing fair information practices. Within the U.S., the direct marketing industry has successfully avoided regulation by arguing that their programs of voluntary self-regulation allow anyone who

chooses to have their name removed from a specific mailing list can contact the individual firm or ask to have their name removed from all national mailing lists by signing up for the Direct Marketing Association's Mail Preference Service. In reality, this is unlikely to be the case. For example, the Direct Marketing Association reported that less than 50 percent of catalogers offer a name-removal option and that only 53 percent of mailers surveyed by the DMA List Council used the Association's Mail Preference Service *(Direct,* 1992; Direct Marketing Association, 1993a). Even individuals who do not participate in direct marketing receive unwanted mail because public records (e.g., motor vehicle records) provide the basis for so many prospect lists, and these lists are sold by large direct marketing firms that have no direct contact with consumers. Clearly, because name removal is key to balancing competing consumer and privacy concerns, the entire issue merits further investigation.

Third, there is a need to develop and validate instruments to measure general attitudes toward various information practices and concern for privacy. In this study, only a small number of items were used to measure attitudes toward direct mail. For example, the reliability for the "prefer mail shopping" sub-scale failed to meet the accepted criterion of a Cronbach alpha of at least .70. The remaining subscales used in this study all consisted of only two items. The Kaiser-Meyer-Olkin Measures of Sampling Adequacy for the two sets of scales were also lower than is desirable. Given that the theoretical approach of this study appears promising, increasing the length of the scales should achieve an acceptable level of reliability (Spector, 1992). Here, only one dimension of privacy, loss of control, was found to be significant in discriminating among positive and negative attitudes toward secondary information use. Smith, et al. (1992) hypothesize that attitudes about information privacy reflect three dimensions: information collection, information management (which includes both accuracy and unauthorized access to personal information), and information use. Future research should investigate how attitudes about different types of secondary information use are related to concerns about the other privacy dimensions.

Finally, the results also provide support for focusing on the specific characteristics of information practices from Table 1 and Figure 1 in future research on secondary information use. More than 60 percent of the subjects hold positive attitudes toward only three POS practices (POS1-POS3), all of which involve receiving offers directly related to the individual's prior purchases. None of these three practices involve profiling, sensitive information, or the acquisition of third-party information. For this sample, where 72 percent of the participants hold positive attitudes toward direct mail in general, Table 6a shows that 60 percent or more of the participants hold negative attitudes toward the majority of the 11 POS practices (POS5-POS10). These practices all involved one or more of the following: acquisition and use of third party-information, use of financial information, profiling, and/or making inferences that some participants viewed as unwarranted or inappropriate. For example, one respondent commented, "It seems that whenever I get something in the mail, it does not apply to me and a company has assumed too much." Another stated, "My privacy is violated when information from one source is merged with another source to get a better profile of me." While these findings are consistent with theory, there is a need in future research to vary these characteristics more systematically using an experimental design. For example, it would be interesting to measure attitudes toward the receipt of offers for "sensitive" products that the individual had previously purchased, such as alcoholic beverages or birth control devices.

In conclusion, until we have a better understanding of the issues raised in this study and can use this understanding to guide practice, companies that collect and use personal information are well-advised to voluntarily observe fair information practices by informing consumers how personal information will be used, providing options about the subsequent use of personal information, and allowing consumers to make an informed choice based on the these options, including a clear opportunity for name removal. The media, state legislatures and attorney generals, and Congress continue to scrutinize both individual companies and industries perceived as engaging in unfair information practices. For example, the Direct Marketing Association reported that as of April 1993, 109 privacy bills affecting personal information use are pending in 29 states (Direct Marketing Association, 1993b). In the past, such legislation at both the state and federal levels has typically included proposals to codify fair infor-

mation practices. For firms wishing to avoid this form of scrutiny, observing fair information practices as a matter of standard practice constitutes policy that is both ethical and pragmatic. Where a firm transfers sensitive information to third parties without the possibility of observing fair information practices, the wise decision may be to discontinue the practice altogether, even when the activity is not prohibited by law, such as with Equifax's 1991 decision to discontinue the sale of mailing lists based on credit reports (Schultz, 1991). Given today's heightened public interest in privacy, the net result for organizations that ignore this message is the likelihood that privacy will continue to remain front page news.

Acknowledgements

The author acknowledges the helpful comments of John Baker, Bob Bies, Dick Mason, Sandra Milberg, Brian Mittman, Joel Reidenberg, Debra Ringold, Jeff Smith, Bob Zmud, and the anonymous *MISQ* reviewers on earlier versions of this paper. Deborah Salmond and Bob Thomas provided good advice on methodology. I have also benefited from discussions with Keith Wardell, Mike Miller, Jim Rule, and Alan Westin, and from participating in the 1992 Roundtable on Secondary Information Use at the John Marshall Law School, Chicago, Illinois. This research was partially supported by a Georgetown School of Business Administration summer research grant.

References

Applegate, L.M. and Wishart, N. *Frito-Lay, Inc: A Strategic Transition (C),* Case 9-190-071, Harvard Business School, Boston, MA, 1990.

Baker, J.A. "Personal Information and Privacy," in *Proceedings of the First Conference on Computers, Freedom and Privacy*, J. Warren, J. Thorwaldson, and B. Koball (eds.), IEEE Computer Society Press, Los Alamitos, CA, 1991, pp. 42-45.

Bates, S. "A Blockbuster Debate About Privacy," *Washington Post*, January 1, 1991, pp. E1-2.

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

Bruns, W.J. and McFarlan, F.W. "Information Technology Puts Power in Control Systems," *Harvard Business Review* (65:5), September-October 1987, pp. 89-94.

Buchwald, A. "Credit Card Sharks," *Washington Post,* June 25, 1992, p. C1.

Burnett, E. *The Complete Direct Mail List Handbook,* Prentice-Hall, Englewood Cliffs, NJ, 1988.

Clarke, R.A. "Information Technology and Dataveillance," *Communications of the ACM* (31:5), May 1988, pp. 498-512.

Cohen, R. "The Rebellion of Private Cohen," *Washington Post Magazine*, April 21, 1991, p. 5.

Commission of the European Communities. *Proposal for a Council Directive Concerning the Protection of Individuals in Relation to The Processing of Personal Data,* Brussels, 1990.

Crenshaw, A.B. "Credit Card Holders to Be Warned of Lists," *Washington Post*, May 14, 1992, p. D11.

Culnan, M.J. "Designing Information Systems to Support Customer Feedback: An Organizational Message System Perspective," in *Proceedings of the Tenth International Conference on Information Systems*, J.I. DeGross, J.C. Henderson, and B.R. Konsynski (eds.), copies available from Association for Computing Machinery, New York, NY, 1989, pp. 305-313.

Culnan, M.J. "Consumer Attitudes Toward Direct Mail, Privacy and Name Removal: Implications for Direct Marketing," paper presented at the Symposium on Consumer Privacy, Chicago/Midwest Direct Marketing Days, Chicago, IL, 1993.

Culnan, M.J. and Smith, H.J. *Lotus MarketPlace: Households . . . Managing Information Privacy Concerns (A) & (B),* case study, School of Business Administration, Georgetown University, Washingon, DC, 1992.

Direct. "Take Your Blinders Off," (4:7), July 1992, p. 1.

Direct Marketing Association. *1991/92 Statistical Fact Book: Current Information About Direct Marketing,* Kendall/Hunt Publishing Company, Dubuque, IA, 1992.

Direct Marketing Association. *1992/93 Statistical Fact Book: Current Information About Direct Marketing,* Kendall/Hunt Publishing Company, Dubuque, IA, 1993a.

Direct Marketing Association. "State Legislation," *Washington Update* (2:3), April 19, 1993b, p. 8.

Dutton, J.E. and Jackson, S.E., "Categorizing

Strategic Issues: Links to Organizational Action," *Academy of Management Journal* (12:1), March 1987, pp. 76-90.

Flaherty, D. *Protecting Privacy in Surveillance Societies,* University of North Carolina Press, Chapel Hill, NC, 1989.

Fusilier, M.R. and Hoyer, W.D "Variables Affecting Perceptions of Invasion of Privacy in a Personnel Selection Situation," *Journal of Applied Psychology* (65:5), October 1980, pp. 623-626.

Gentile, M. and Sviokla, J.J. *Information Technology in Organizations: Emerging Issues in Ethics & Policy,* note, Harvard Business School, Boston, MA, 1990.

Goldstein, R. *The Cost of Privacy,* Honeywell Information Systems, Brighton, MA, 1975.

Hair, J.E., Jr., Anderson, R.E., and Tatham, R.T. *Multivariate Data Analysis,* 2nd edition, Macmillan, New York, NY, 1987.

Ives, B. *The Tom Thumb Promise Club,* case study, Cox School of Business, Southern Methodist University, Dallas, TX, 1989.

Jackson, S.E. and Dutton, J.E. "Discerning Threats and Opportunities," *Administrative Science Quarterly* (33:3), September 1988, pp. 370-387.

Katz, J.E. and Tassone, A.R. "Public Opinion Trends: Privacy and Information Technology," *Public Opinion Quarterly* (54:1), Spring 1990, pp. 125-143.

Laufer, R.S. and Wolfe, M. "Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory," *Journal of Social Issues* (33:3), Summer 1977, pp. 22-42.

Laufer, R.S., Proshansky, H.M., and Wolfe, M. "Some Analytic Dimensions of Privacy," in *Environmental Psychology: People and Their Physical Settings,* 2nd edition, H.M. Proshansky, W.H. Ittelson, and L.G. Rivlin (eds.), Holt, Rinehart and Winston, New York, NY, 1976, pp. 206-217.

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

Loch, K.D., Carr, H.H. and Warkentin, M.E. "Threats to Information Systems: Today's Reality, Yesterday's Understanding," *MIS Quarterly* (16:2), June 1992, pp. 173-186.

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

Louis Harris and Associates, Inc. *Harris-Equifax Consumer Privacy Survey 1992,* Equifax Inc., Atlanta, GA, 1991.

Louis Harris and Associates, Inc. *Harris-Equifax Consumer Privacy Survey 1992,* Equifax Inc., Atlanta, GA, 1992.

Louis Harris and Associates, Inc. and Westin, A.F. *The Dimensions of Privacy: A National Opinion Research Survey of Attitudes Toward Privacy,* Garland Publishing, Inc., New York, NY, 1981.

Mason, R.O. "Four Ethical Issues of the Information Age," *MIS Quarterly* (10:1), March 1986, pp. 4-12.

Miller, A. *The Assault on Privacy: Computers, Data Banks and Dossiers,* University of Michigan Press, Ann Arbor, MI, 1971.

Miller, M.W. "Coming Soon to Your Local Video Store: Big Brother," *Wall Street Journal,* December 26, 1990, pp. 9-10.

Miller, M.W. "Hot Lists: Data Mills Delve Deep to Find Information About Consumers," *Wall Street Journal,* March 14, 1991, p. A1.

Plesser, R.L. and Cividanes, E.W. *Privacy Protection in the United States: A 1991 Survey of Laws and Regulations Affecting Privacy in the Public and Private Sector,* Piper & Marbury, Washington, DC, 1991.

Porter, M.E. and Millar, V.C. "How Information Gives You Competitive Advantage," *Harvard Business Review,* (63:4) July-August 1985, pp. 149-160.

Privacy Protection Study Commission. *Personal Privacy in an Information Society,* U.S. Government Printing Office, Washington, DC, 1977.

Reidenberg, J.R. "Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?" *Federal Communications Law Journal* (44:2), March 1992, pp. 195-243.

Schoeman, F.D. "Privacy: Philosophical Dimensions of the Literature," in *Philosophical Dimensions of Privacy: An Anthology,* F.D. Schoeman (ed.), Cambridge University Press, Cambridge, United Kingdom, 1984, pp. 1-33.

Schultz, R. "Equifax Bites the Bullet," *DM News,* August 12, 1991, p. 38.

Sherman, R. Statement of the Direct Marketing Association before the New York State Consumer Protection Board, June 11, 1992.

Simitis, S. "Reviewing Privacy in an Information Society," *University of Pennsylvania Law Review* (135:3), March 1987, pp. 707-746.

Smith, H.J. "Information Privacy Policies and

Practices: Inside the Organizational Maze, *Communications of the ACM,* forthcoming.

Smith, H.J., Milberg, S., and Burke, S. "Concern for Privacy Instrument," working paper, School of Business, Georgetown University, Washington, DC, 1992.

Smith, R.E. "Target Marketing: Turning Birds of a Feather into Sitting Ducks," *Business and Society Review,* Winter 1991, pp. 33-37.

Spector, P.E. *Summated Rating Scale Construction: An Introduction,* Sage, Newbury Park, CA, 1992.

Stone, E.F. and Stone, D.L. "Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms," in *Research in Personnel and Human Resources Management,* Volume 8, K.M. Rowland and G.R. Ferris (eds.), JAI Press, Inc., Greenwich, CT, 1990, pp. 349-411.

Stone, E.F., Gardner, D.G., Gueutal, H.G., and McClure, S. "A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations, *Journal of Applied Psychology* (68:3), June 1983, 459-468.

Straub, D.W. and Collins, R.W. "Key Information Liability Issues Facing Managers: Software Piracy, Proprietary Databases, and Individual Rights to Privacy," *MIS Quarterly* (14:2), June 1990, pp. 143-156.

Tolchinsky, P.D., McCuddy, M.K., Adams, J., Ganster, D.C., Woodman, R.W., and Fromkin, H.L. "Employee Perceptions of Invasion of Privacy: A Field Simulation Experiment," *Journal of Applied Psychology* (66:3), June 1981, pp. 308-313.

U.S. Department of Health, Education and Welfare. *Records, Computers and the Rights of Citizens,* Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Massachusetts Institute of Technology, Cambridge, MA, 1973.

Vidmar, N. and Flaherty, D. "Concern for Personal Privacy in an Electronic Age," *Journal of Communication* (35:2), Spring 1985, pp. 91-103.

Warren, S.D. and Brandeis, L.D. "The Right to Privacy," *Harvard Law Review* (4:5), March 1890, pp. 193-220.

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

Westin, A.F. "Domestic and International Data Protection Issues," in *How the American Public Views Consumer Privacy Issues in the Early 90's—and Why,* testimony before the Subcommittee on Government Information, Justice, and Agriculture, Committee on Government Relations, U.S. House of Representatives, U.S. Government Printing Office, Washington, DC, 1991, pp. 54-68.

White, J.R. "President's Letter," *Communications of the ACM* (34:5), May 1991, pp. 15-16.

Woodman, R.W., Ganster, D.C., Adams, J., McCuddy, M.K., Tolchinsky, P.D., and Fromkin, H. "A Survey of Employee Perceptions of Information Privacy in Organizations, *Academy of Management Journal* (25:3), October 1982, pp. 647-663.

Yeck, J.D. "Editorial: DM > DO," *Journal of Direct Marketing* (6:1), Winter 1992, pp. 2-3.

About the Author

Mary J. Culnan is associate professor in the School of Business at Georgetown University. She holds a Ph.D. in management from the University of California, Los Angeles. Her research has been published in *MIS Quarterly, Management Science, Organization Science, Decision Sciences,* and the *Journal of the American Society of Information Science*. Her current research focuses on consumer attitudes toward privacy and direct marketing. Dr. Culnan has testified before the U.S. House of Representatives on information policy issues on several occasions. During the spring of 1993, she served on a White House Task Force on Presdential Correspondence.

Appendix

Questionnaire for 11 POS Items

Assume you have joined a "shoppers club" at the local grocery store (such as the Safeway Savings Club). You receive coupons and other offers in the mail in exchange for letting the store record your purchases when you check out. The store then knows what products each member of the club has purchased.

When you sign up for the program, you are asked to provide your name and address, your home and work telephone numbers, your social security number, and the number of people in your household.

The membership application includes this statement: "I understand and agree that the store may record, make use of and disclose to other persons or entities any and all of the information I furnish on this application form and information about the products I purchase as a member of the savings club."

The grocery store *only provides names and addresses* to other companies. Other personal information they have collected about you is *not shared* with other companies.

Please indicate your feelings about the following uses of your personal information by circling the appropriate number on the scale following each description. For all questions, *assume you actually purchased* the products in the question.

[NOTE: All items scaled identically. In the interest of space, the scale is only shown for the first item]

1. You receive coupons in the mail for products you have previously purchased. How do you view this use of personal information?

    1. Primarily useful
    2. Rarely useful but do not see a problem
    3. More as a nuisance
    4. More as an invasion of privacy

2. You regularly buy Diet Coke. You receive coupons in the mail from Pepsi-Cola for Diet Pepsi. How do you view this use of personal information?

3. You always buy your favorite magazine at the grocery store. The magazine publisher buys a *list of names and addresses* of people who purchased its magazine at the grocery story and *mails you an offer* to subscribe to the magazine at a special rate. How do you view this use of personal information?

4. Because you buy lots of natural foods, the grocery store has classified you as someone who is "health-conscious." An *environmental group* buys a *list of names and addresses* of "health-conscious" shoppers and sends you an application for membership. How do you view this use of personal information?

5. Because you frequently buy low calorie foods, the grocery store has classified you as someone who is "weight-conscious." *Weight Watchers* buys a *list of names and addresses* of these "weight-conscious" shoppers and sends you literature about their weight loss programs. How do you view this use of personal information?

6. The company you work for is concerned that drinking alcohol is bad for health. It buys a *list of names and addresses* of shoppers who have purchased beer or wine from the grocery story and *matches these names and addresses* against the names and addresses of its employees. It mails you a letter from the company president about the health risks of alcohol abuse. How do you view this use of personal information?

7. A dating service for single people buys a *list of names and addresses* of shoppers who regularly buy "single serving" products (such as Soup for One) and *mails you a questionnaire* about your "ideal date." How do you view this use of personal information?

8. Your credit card company sells information about its customers (purchasing power, estimated income) to the grocery store. The *grocery store merges information* about your credit card account with your purchase information in the grocery store database. How do you view this use of personal information?

9. The *grocery store uses the information it acquired from the bank* to categorize shoppers based on their income. The store begins to mail different offers to shoppers based on their income. For example, it sends an offer for "double coupons" to "low income" people only. How do you view this use of personal information?

10. A *direct marketing company sells personal information* compiled from 22 different sources (such as type of vehicle owned, whether or not a person shops by mail or has a credit card) to the grocery store. The *grocery store merges* this additional information with your purchase information in the grocery store database. How do you view this use of personal information?

11. The grocery sells a *book club* a *list of names and addresses* of shoppers who have bought paperback books and gourmet foods at the grocery store, who shop by mail, and also drive a foreign car. The *book club mails* you a promotional offer. How do you view this use of personal information?