GLEN J. NOWAK
JOSEPH PHELPS

Direct Marketing and the Use of Individual-Level Consumer Information: Determining how and When "Privacy" Matters

GLEN J. NOWAK is an associate professor in the College of Journalism and Mass Communication at the University of Georgia. He has a PhD and an MA from the University of Wisconsin. His research interests include direct response TV advertising, the impact of direct marketing on consumers' privacy, and advertising effects on consumer behavior.
JOSEPH E. PHELPS is an assistant professor in the Advertising and Public Relations Department at the University of Alabama. He has a PhD and an MA from the University of Wisconsin. His research interests include consumer perceptions of direct marketing and privacy issues, children's responses to TV advertising, and examining the implications of integrated marketing communications on current marketing practices, theory, and research.

ABSTRACT

The desire to maximize marketing effectiveness and reduce communication costs has increased direct marketers' reliance on computerized databases, customized persuasion, and other consumer information intensive strategies and tactics (28,541. The belief that the success of marketing efforts is positively related to the amount and specificity of individual-level consumer information (7). however, has raised questions about how far companies should be allowed to go in learning about or attempting to persuade consumers (6.40). In the process, privacy has become widely evoked, but often elusive concept. This article develops a framework for addressing privacy concerns that arise when direct marketers utilize consumer information. It does so by identifying the underlying dimensions of the privacy construct and examining the relationships between those dimensions and direct marketers' consumer information practices. This approach not only helps identify situations when privacy matters. but suggests productive strategies and tactics for alleviating consumer concerns related to the use of individual-level consumer information.

CCC 0892-0591/97/040094-15

INTRODUCTION

Spurred by advances in computer and database technologies, an ever-increasing number of direct and general marketers believe that the effectiveness of marketing communication strategies is directly related to the amount and specificity of consumer information (7, 38). Whereas marketers traditionally relied upon or were only able to obtain relatively broad geographic, demographic, and psychographic information, today it is possible to formulate positioning, message, and media strategies using personal (i.e., individual-level) consumer information (10, 59). According to recent estimates, about 20,000 commercial and public databases are available to marketers, with over 450 companies generating most of their sales revenue from the provision of an ever-increasing amount of personal information (6, 34). These data are either obtained directly from consumers as a result of the marketing exchange process (e.g., mail or telephone orders, loyalty clubs, product warranty cards, replies *to* direct response ads, sweepstakes promotions, or rebate or mail-in redemption offers), or compiled from public records and government databases (37). By merging different databases and using sophisticated data manipulation techniques, it is possible to develop profiles that reveal an enormous amount of information regarding an individual consumer's personal characteristics, lifestyle, and political and social activities (30).

While advances in database technology and greater access to individual-level information have unquestionably improved direct marketers' market segmentation, media selection, message formulation, and campaign evaluation capabilities, these developments also have raised questions regarding how far companies should be allowed to go in learning about or attempting to persuade consumers (21, 47, 58). Among those who have considered these questions, some (e.g., 17, 30, 42) suggest that while direct marketers are voracious users of individual-level consumer information, relatively few practitioners have considered whether their information practices may adversely affect consumers, and even fewer have tried to differentiate potentially harmful or threatening practices from those that are not.

Public opinion polls, however, indicate that consumers are very concerned about what companies know about them, how companies obtain information, what companies do with the information they collect, and the accuracy of the information they use (12, 15, 32, 48). For instance, 78 percent of the respondents in a 1991 Gallup survey described themselves as "very" or "somewhat" concerned about what marketers know about them (27). Sixty-nine percent of the respondents in a 1991 Time-CNN survey indicated concern over the amount of personal information collected by companies that market products (34), while 68 percent favored prohibiting the sale of product purchase information. Recent national surveys commissioned by Equifax have found most consumers believe they have "lost all control over how personal information about them is used by companies" (24-26), and a recent Louis Harris survey found considerable support for privacy protection measures, with the percentage believing such measures important ranging from 77 percent for the direct mail industry to 94 percent for banks, hospitals, and insurance companies (1).

Although existing federal privacy laws primarily protect individuals from governmental abuses (for a more complete review of laws and regulations, see 2, 49), consumer concerns have been the driving force behind recent legislative attempts to limit or regulate marketers' gathering and use of individual-level information (6, 31). At least 10 federal bills and more then 1,000 state legislative bills related to privacy were presented in 1992 alone, including bills that would prohibit contacting consumers without prior express consent, make prospecting illegal, subject list rental and exchanges to large surcharges that would make them prohibitively expensive, and reduce access to motor vehicles lists (2).

Even if the likelihood of such sweeping legislation being passed is remote, market forces and increased competition on the basis of privacy sensitivity will require direct marketers to address the privacy concerns that arise from the gathering, manipulation, and use of individual-level consumer information (1, 67). Similarly, with Internet and computer on-line services becoming increasingly popular, the need to develop rules and standards for protecting consumer privacy will become more, rather than less, critical in the near future. More

than traditional direct marketers, on-line service companies and other firms using interactive technologies are well equipped to track exactly what consumers are doing in cyber space, including what they stop to look at, what they buy, what they inquire about, and what they read (44). Regardless of the realm, it is clear that vague and overly broad conceptualizations of privacy represent one of the primary hurdles to formulating policies that balance consumer concerns with direct marketers' legitimate business interests. Thus, a necessary first step in developing appropriate information rules or standards is a clear understanding of what "privacy" is as it relates to direct marketing practices.

This article applies both legal and consumer perspectives to develop suggestions for addressing privacy concerns that arise when direct marketers utilize consumer information. It does so by identifying the underlying dimensions of the privacy construct and examining the relationships between those dimensions and direct marketers' consumer information practices. This approach not only helps identify situations when privacy matters, but suggests productive strategies and tactics for alleviating consumer concerns related to the use of individual-level consumer information.

DEFINING PRIVACY AND ITS RELEVANT DIMENSIONS

Although privacy has been a concept widely used by consumers, consumer advocates, politicians, and direct marketing practitioners (4, 18, 20, 30, 31, 41), its use has not produced a universally agreed upon definition or meaning. Furthermore, privacy is not a right explicitly granted in the U.S. Constitution. It is a concept that has evolved as a legal privilege whose foundation originates in the due-process guarantees of the First, Ninth, and Fourteenth Amendments to the Constitution. In *Griswold et al. v. Connecticut* (1965), for instance, the U.S. Supreme Court ruled that a Connecticut statute forbidding the use of contraceptives violated the right of marital privacy "which is within the penumbra of specific guarantees of the Bill of Rights" (22). Similarly, in *Katz v. United States* (1967), the Supreme Court held that "the Fourth Amendment protects people, not places and if there was a reasonable expectation of privacy then what [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected" (33).

The end result, however, is confusion rather than clarity regarding the privacy concept. To some, "privacy" is a problematic, conceptually murky, and constitutionally questionable concept that. direct marketers should ignore or dismiss on the grounds that it is "a vague right with little legal basis" (50: 74). To others, it is a legally grounded, multifaceted concept that encompasses diminished individual autonomy and anonymity, invasions of personal space and solitude, and the ability to limit or control information access and use (20, 55). Stone and Stone (61) enumerated more than 2,100 books, articles, legal cases, technical reports, and other published documents defining and dealing with the topic of information privacy. Fortunately, the evolution of the privacy construct suggests that there are at least three conceptualizations that have considerable relevance for direct marketers' consumer information practices.

The first perspective dates back to Warren and Brandeis, who in an 1890 *Harvard Law Review* article, articulated privacy as a distinct legal right, specifically, "the right to be let alone" (64:69) [although according to Bigelow (5), this notion originated from Michigan Supreme Court Justice Thomas M. Cooley]. This view, while often found too-broad and vague to provide much practical or legal guidance, is pertinent for two reasons. First, this seminal definition of privacy recognized that the concept encompasses an individual's desire for physical seclusion or solitude. A loss of privacy thus occurs "when the limits one has set on acquaintance with his personal affairs are not respected" by others (23:l); a perspective often shared by recipients of uninvited and unwanted direct mail and telephone solicitations. Second, and more importantly, this definition provides the basis for many of the common-law principles that recognize privacy as an individual right worth granting and protecting (2). Warren and Brandeis's conceptualization of privacy, for example, not only furthered the common-law trend toward acknowledging nonphysical injuries such as harm to reputation, it provided an early

foundation for the assertion that a person should own the "facts relating to his private life" (43:76).

In another perspective, of even greater significance to direct marketing, the elements of seclusion and personal information ownership have become key tenets of many recent efforts to define privacy with regard to modern information practices. Westin's (1967:7-8) seminal view, for instance, defined privacy as the "claim of individuals, groups, or institutions to determine for themselves, when, how, and to what extent information about them is communicated to others." Not only has this definition provided a framework for the Privacy Act of 1974 and the Fair Credit Reporting Act of 1982, it has shaped recent discussions regarding information privacy. For example, Stone and Stone (62) characterized privacy as a state or condition in which an individual has the ability to (a) control the release or subsequent dissemination of information about him or herself, (b) regulate the amount and nature of social interaction, and (c) exclude or isolate himself or herself from unwanted auditory or visual stimuli. Similarly, Culnan (in press), in an examination of consumer attitudes toward mail and telephone solicitations, defined privacy as "the ability of individuals to control the access others have to personal information about them." From this perspective, unwanted direct mail or telemarketing calls are symptoms that arise from the inability to control the secondary use of personal information by third parties.

Finally, despite its contentious constitutional standing, court rulings, scholarly and legal discussions, and legislative actions have codified the notion that privacy is not a unified or singular concept, but instead is a term that encompasses a number of distinct rights. Dickler (13), for instance, suggested that the privacy concept embraces three such rights: "a right to publicity," which bars the unauthorized appropriation of one's name or image; a "right of seclusion," which shields people from unwanted intrusions; and a "right to keep private facts private." This perspective was expanded by Prosser (53), who proposed that privacy encompassed four separate and discrete legal torts: (a) intrusion (i.e., physically invading a person's seclusion or solitude; (b) disclosure (i.e., publicly disclosing embarrassing private facts); (c) false light (i.e., false public portrayals); and (d) appropriation (i.e., use of a person's image or identity without permission). In other words, "private facts" encompassed two distinct categories: one in which the facts were private but the plaintiff's reputation was unharmed, and a second in which the information revealed was misleading and put the plaintiff in a "false light" (43).

Thus, applied to direct marketing, the preceding conceptualizations of privacy have two important implications. One, they severely reduce, if not completely eliminate, the applicability of privacy, at least from a legal perspective, to information practices that use group-level or non-individual specific data. Group-level information emanates from the marketers rather than the consumer (e.g., the marketer uses secondary sources), involves generalizing across groups of consumers (e.g., Simmons Market Research Bureau reports, where the focus is on market segments not individual consumers), often involves inferring characteristics and behaviors using such broad indicators as geography and demographics (e.g., VALS, PRIZM, and other clustering approaches), and usually necessitates making more as well as broader assumptions about consumers (e.g., PRIZM, which assumes people are like their neighbors). It is thus possible for marketers to conduct targeted advertising campaigns without knowing the names of specific consumers or without relying on a database that contains the profiles of individual consumers. Conversely, individual-specific information refers to data that pertain, or specifically relate, to a single identifiable person. Credit and financial histories, customer files, license applications, and vehicle registration lists, for example, all identify individual consumers and provide information and facts (e.g., height, weight, annual income, past purchases) specific to that person. For privacy to be legally viable, the information practice or issue must involve individual-level consumer information (i.e., personal information that is traceable or directly concerns a given, named individual). Second, they suggest that addressing information privacy issues requires: (a) identifying the relevant privacy dimension(s), and (b) considering the information practice within that dimension's well-defined context. This process, when applied to direct marketing, not only suggests that some dimensions have more relevance than others, but illustrates the difficulties inherent in relying on

legalistic frameworks to address consumer privacy concerns.

APPLYING PROSSER'S (53) FRAMEWORK TO DIRECT MARKETING

Since Prosser's four-part analysis has been accepted by nearly all courts and embraced by federal laws (43) it provides a useful and highly relevant framework for evaluating direct marketers' practices relating to the gathering and use of individual-level consumer information. From both a historical and judicial perspective, direct marketers' information practices stand up quite well with respect to three of Prosser's torts: intrusion, disclosure, and false light.

Despite consumer complaints about the reception and/or volume of unwanted direct mail and telemarketing solicitations, at least two factors considerably reduce the legal relevance of the intrusion dimension of privacy to direct marketing. First, even though some data-gathering practices take place inside consumers' homes (e.g., television viewing research) or involve physical measures (e.g., eye tracking or galvanic skin responses), the knowing and willing cooperation of consumers (i.e., the research participants) eliminates the primary basis for an intrusion claim. The fact that the individual data or responses are typically summarized and presented at a group level further reduces intrusion's applicability. Second, despite some recent civil actions against telemarketers [e.g., Robert Bulmash's financial compensation requests from companies warned against unwanted solicitations (45)], legal reviews of the evolution of privacy indicate that the concept of intrusion has been primarily confined to privacy issues involving a person's physical being *(e.g., Roe v. Wade,*1973 striking down prohibitions against abortion) (l6, 43). To be actionable in other contexts (e.g., the home), the intrusion, whether physical (e.g., examining the contents of a purse) or nonphysical (e.g., wiretapping), the area invaded must truly be private, there must be no valid reason for the intrusion, and the intrusion itself must be highly offensive to a reasonable person (43).

Prosser's second tort, public disclosure, operates within similarly narrow parameters that would exclude most direct marketing practices. At a minimum, the private facts about the individual must be of a kind that, when disclosed without permission, would be "highly offensive and objectionable" to a person of ordinary sensibilities (40). In most instances, however, First Amendment or free speech protections supersede any privacy claims. In cases brought against newspapers, which are usually a more public medium than direct mail, courts have recognized that publication of personal information infringes upon privacy interests but ruled for defendants under "public figure" or "news of general interest" exceptions (43). The gathering and dissemination of individual-level information related to sexual relations or personal illnesses with negative connotations (e.g., AIDS), however, increases the viability of disclosure claims. Furthermore, depending on the relationship between the individual and the disclosing party (e.g., doctor-patient), a legal basis for confidentiality claims may exist (56).

Consumers concerned about the accuracy of direct marketers' data files are also likely to find it difficult to pursue false light actions successfully. Along with showing harm, plaintiffs must again persuade the courts that privacy concerns outweigh free speech considerations. Public figures suing the news media, for instance, must prove not only that a publication was false and hurt their reputation, but that the medium acted with malice, or reckless disregard of the truth (43). Although the U.S. Supreme Court has not yet held that private figures who prove damages and fault need also prove malice in libel suits against the media, there may be more productive ways to address the harms to image or reputation that result from the publication or dissemination of false or inaccurate individual-level information. McWhirter and Bible (43), for instance, suggested both the law of defamation, which protects reputations, and the "intentional infliction of mental distress" tort, which affords relief to those who suffer mental distress at the hands of people who should have known that their acts might cause such distress, as more appropriate legal venues. A recent case involving a Trans Union Credit Information Co. credit report, however, may shed more light on the legal viability of false light claims. In January 1995, the 9th U.S. Circuit Court in San Francisco reinstated a lawsuit against Trans Union that

was filed by woman who claimed uncorrected credit errors in her credit report caused her anguish and kept her from applying for credit (66).

Prosser's fourth tort, appropriation, thus appears to the privacy dimension most directly related to direct marketers' gathering and use of individual-level information. Evolving from the early "right of publicity" cases, this dimension of the privacy concept has the strongest, most widely accepted, legal foundation. First, in *Zacchini v. Scripps-Howard Broadcasting* (1977) the Supreme Court ruled that appropriation (i.e., the unauthorized commercial use of one's name or image), is an invasion of a person's privacy. In the case, Zacchini, who performed an act in which he was shot from a cannon into a net some 200 feet away, alleged Scripps-Howard unlawfully appropriated his professional property by videotaping and showing his act in its entirety on a television news program. The Court, citing *Housh v. Peth* (1956), ruled that

> an actionable invasion of privacy is the unwarranted appropriation or exploitation on one's personality, the publicizing of one's private affairs with which the public has no legitimate concern, or the wrongful intrusion into one's private activities in such a manner as to outrage or cause mental suffering, shame, or humiliation to a person of ordinary sensibilities. (69: 562)

Second, a logical basis exists for expanding the appropriation dimension of privacy to encompass direct marketing practices that involve the use or dissemination of individual-level information, such as list renting or sharing. In general, the argument is just as an individual retains some control over reproductions of their physical likeness and the ways it can be used by others (i.e., is entitled to give, sell, or withhold permission of its use), that individual also should be able to retain and exercise control over database representations or specific personal facts provided by the individual in the course of a business transaction. Furthermore, as Posch (50:74) noted, consumers-the group most affected by direct marketers' information gathering and use practices-typically define privacy as "the ability to restrict the use of information about himself or herself or restrict access to the same." Not surprisingly, empirical research to date has found consumer privacy concerns highest for practices involving secondary uses of information without prior consent (e.g., a magazine publisher rents its list to a catalog marketer), with 80 percent of the respondents in one survey labeling the practice of renting personal information to other companies a "serious" invasion of privacy (48).

DIRECT MARKETERS' INFORMATION PRACTICES: WHEN PRIVACY MATTERS

Overall, the application of Prosser's conceptualization of privacy provides considerable direction for direct marketers. First, taking the narrowest perspective, Prosser's framework suggests that from a legal standpoint, only two dimensions of the privacy concept-disclosure and appropriation-may be of real concern to direct marketers. Furthermore, in the case of disclosure, direct marketers' information practices may be actionable only to the extent they are widely and inappropriately disseminating highly personal information regarding the specific financial, medical, or sexual relations of individually identified consumers. Claims or concerns related to other categories of consumer information, such as demographics or lifestyle activities, are not likely to be deemed "highly offensive and objectionable" to a person of ordinary sensibilities. Expanding outward from that narrow perspective, however, Prosser's framework also illustrates that greater definitional specificity is necessary to address information privacy issues. Given the continual (and usually willing) provision of personal information *as* part of the exchange for goods and services, it is more appropriate to view privacy as a multidimensional concept. In the modern day world of marketing, it is no longer feasible, as Turn (65:28) noted, to characterize privacy under such unidimensional definitions as "the right to be left alone" or "the right to unilaterally control information about oneself."

Most importantly, though, the application of Prosser's framework to direct marketing demonstrates the value of going beyond strictly legal considerations when it comes to addressing consumers' privacy concerns. Such an approach, while useful for addressing the question of whether consumers

have constitutionally protected privacy rights, places emphasis on the legal viability of invasion of privacy claims to the exclusion of more relevant marketing considerations such as marketplace sentiments, consumer desires and satisfaction, and the overall quality of consumer relationships. In other words, privacy, when considered in a broader context, involves explicit and implicit social contracts in which individuals exchange a measure of privacy for some economic or social benefit (35, 46). Thus, just as conceptualizations of privacy need to recognize its multifaceted nature, efforts to address consumer privacy concerns must go beyond reliance on a singular perspective-however useful and instructive that perspective may be.

One approach, advocated by Turn (65:28), is to specify "the rights of individuals regarding the collection, storage, processing, dissemination, and use of personal information about them." Although Turn did not identify what those rights may be, her perspective recognizes that individual-level information often passes through a series of stages, with each stage having unique privacy implications. Alleviating consumer privacy concerns, and finding a balance between those concerns and marketers' legitimate needs for information, involves specifying each party's information rights. In the case of direct marketing, the adoption of such a process best begins with examining what happens at the two stages that attract most of the consumer concern: the initial gathering of information and its ultimate use.

Data Gathering and Privacy

As Figure 1 illustrates, direct marketers use a variety of methods to gather individual-level information, and the conspicuousness and obtrusiveness of these methods varies greatly. As the matrix shows, direct marketers' data-collection methods can be classified using five general categories, while consumers' knowledge of the method employed typically falls into one of three categories: full knowledge of data collection and data use(s), knowledge of collection but not of use(s), and ignorance of both collection and use(s). If a data-collection method is readily apparent (e.g., participating in a consumer survey), requires a priori consumer consent, and is based on voluntary consumer participation, it can be assumed consumers knew information about them was collected. Assuming consumers also are made aware of all subsequent uses of the information, privacy, from a legal, social, or ethical standpoint, is not an issue. In most cases, the individual-level information was willingly supplied in expectation of such future benefits as reduced prices, premiums, or other incentives. In cases where consumers would prefer not to provide personal information but do so because the market exchange requires it, privacy concerns are alleviated by the voluntary nature of the transaction as well as by advising consumers of the information's collection and uses.

As Figure 1 shows, the data-gathering practices that are most likely to threaten consumer privacy occur in Columns 2 and 3. Here, individual-level information is gathered either with the knowledge or active consent of consumers and then used in ways consumers have little or no knowledge of, or without consumers' consent *and* without consumers knowing how the information will be used. The most common direct marketing instances where consumers have knowledge of collection but often not of use(s) include promotional offers involving toll-free telephone numbers or mail-in premiums or rebates, warranty cards, and membership applications sent directly to marketers, and market, audience, or consumer research studies and surveys. In each case, consumers are voluntarily and knowingly providing marketers with individual-level information, and often know the primary purpose of the data collection or the primary uses of the information. However, as Figure 1 shows, there are a number of instances where the information is gathered for one purpose (which consumers are aware of) and then used for other purposes (which most consumers are not aware of). These situations commonly occur when the information is obtained through secondary sources or when companies other than the original marketer gain access to the information *as* a result of being involved in the exchange process (i.e., incidental users).

Secondary source data refer to individual-level information that does not come directly from the consumer to the marketer. Rather, such data result from direct marketers sharing information with other marketers or emanates from publicly accessible databases. Many direct marketers, for instance, rely on personal and household information gathered by federal, state, and local governments, in-

Collection Method	Relative Level of Consumer Knowledge		
	Full Knowledge of Collection and Use	Knowledge of Collection Rather than Use	Ignorance of Collection and Use
Time/Place of Purchase	Scanner Data Frequent Flyer Programs Frequent Buyer Programs Magazine Subscriptions Catalog Purchases/Orders Financial Transactions	Scanner Data Frequent Flyer Programs Frequent Buyer Programs Magazine Subscriptions Catalog Purchases/Orders Financial Transactions	Magazine Subscription Catalog Purchases Surveillance Cameras Financial Transactions
Telephone Inquiry	Screening/Qualifying Calls Calls to 800 numbers Calls to 900 numbers	Screening/Qualifying Calls Calls to 800 numbers Calls to 900 numbers	Automatic Number Identification (ANI) Calls to 800 numbers Calls to 900 numbers
In Response to Advertising or Promotion Offers	Coupons Trial Offers "Free" Offers Premium Offers Warranty Cards Membership Clubs	Coupons Trial Offers "Free" Offers Premium Offers Warranty Cards Membership Clubs Newsletters	Electronic or interactive response devices that don't inform consumers that information is being collected and stored for later uses.
Surveys, Studies, and Questionnaires	U.S. Census Media Use Surveys Consumer Shopping Panels	U.S. Census Media Use Surveys Consumer Shopping Panels	
Public/ Proprietary Databases	Public Records Vehicle Registrations Postal Records List Brokers/Compilers Telephone Directories	Public Records Vehicle Registrations Postal Records List Brokers/Compilers Telephone Directories	Postal Records List Brokers/Compilers

FIGURE 1
Direct Marketers' Information Collection Methods and Consumer Knowledge of Information Collection and Use

cluding U.S. Census data, vehicle registration records, driver and marriage license files, birth and death certificates, and property ownership records (19). Incidental users, on the other hand, obtain access to individual-level information by assisting in the transaction between the marketer and the consumer. The most common incidental users in the marketing and advertising context are 800 phone number providers, order fulfillment companies, shipping firms, financial transaction processors, and credit card issuers (39).

From a consumer as well as legal perspective, appropriation is the only potentially relevant privacy dimension when individual-level information gathered in one context is later used in unknown, or quite distant, marketing contexts. Appropriation is applicable in that it encompasses information control, which consumers may lose in one of two ways. First, control is reduced to the extent that ignorance of information uses decreases consumers' ability to forego participation or to limit what information about them is distributed and used. Second, if *Zacchini v. Scripps-Howard Broadcasting* (1956) is a relevant guide, the use of secondary or incidentally collected information could be challenged as an unwarranted appropriation or exploitation of one's personality (69). It is difficult to conceive marketing practices causing mental suffering, shame, or humiliation to a person of ordinary sensibilities, but it could be argued that many marketing information

practices are based on the erroneous assumption that marketers have a right to use individual-level information in any manner they desire. It also appears that incidental users are most vulnerable to such a claim since their "rights" to keep and use the data they collect are often tenuous, particularly from the perspective of the companies who have hired them as intermediaries (3, 39).

Privacy becomes a more meaningful concern, however, when consumers lack knowledge of the information collection and therefore, its actual use(s) (17). These situations typically occur when completely surreptitious data-collection methods such as surveillance cameras, automatic telephone number identification (ANI) systems, or electronic record-keeping systems are used. Ignorance of data collection and use also applies to situations involving information compiled by firms that, from a consumer perspective, are so incidental as to never be suspected (e.g., a delivery company that tracks customer names and firms ordered from). Although direct marketers employ few completely surreptitious data-collection methods (see Figure 1), the expanded availability of AN1 systems makes this an important source of consumer privacy concerns. Publicity over the availability of Caller ID, a similarly structured residential service, has increased public awareness of such systems, but few consumers are aware that almost every 800 or toll-free number automatically identifies incoming callers' phone numbers (9, 28, 63). Even fewer are aware of marketers' ability to link ANI systems with databases that contain other personal information-income, credit history, and marital status-usually without the caller's consent or knowledge. Privacy is thus a relevant concept in at least three ways. First, appropriation is applicable in that the use of such systems places information control in marketers' rather than consumers' hands. Marketers, without input from consumers, decide when information will be collected and what pieces of individual-level information will be accessed (and therefore used as a representation of the caller). Appropriation is also relevant in that consumers, without their knowledge or input, can be classified or defined in ways that, regardless of the level of accuracy, reduce individual autonomy (11). Finally, caller identification systems ensure that consumers who directly respond to advertising offers have no way, short of using a pay phone, to preserve their anonymity or impede the amount of information collected about them. Many companies, in fact, rarely disclose the use of ANI systems to avoid raising such privacy concerns (9).

Information Use and Privacy

An examination of the data-gathering practices gives a better indication of how direct marketers' information practices affect consumers' privacy, but such an assessment is incomplete. The relevance of the privacy construct is also dependent on how the data is used as well as the level of information specificity. Furthermore, it is the interaction of these two general factors that often determines when, and how, privacy matters (see Figure 2).

As Figure 2 illustrates, marketers typically use consumer information in three major ways: (a) to segment or profile markets and audiences; (b) to create, personalize, or direct persuasive messages and advertising; and (c) for financial gain (i.e., renting or selling the information to others). It is important to note that the privacy implications relating to each of these applications differ greatly depending on whether one adopts a relatively narrow legal perspective or a broader consumer-based view. From a consumer perspective, concerns have been raised over each of these applications, regardless of whether individual-level and group-level information was used. Figure 2 illustrates potential privacy threats from the consumer perspective. From the legal perspective, although each of these applications conceivably has privacy implications, the applicability of the privacy construct is highly dependent upon the specificity of the information involved. Much consumer information used by marketers, for example, involves group-level, rather than individual-level, consumer information.

As Figure 2 illustrates, when it comes to data use, the greatest potential threats *to* consumer privacy involve information that is directly associated with specific individuals. From a legal perspective, when group-level or generalized data are used, the privacy of individual consumers is essentially unaffected by marketing practices. For example, if a marketer uses an approach such as VALS to profile an audience, it is likely that the inferences made when applying that approach will result in some consumers being placed in inappropriate categories. From a legal perspective, though, such a misclassification is be-

Level of Information Specificity	Data Uses/Applications		
	Market and Audience Segmentation or Profiling	*Media Planning and Message Design*	*Selling/Renting Consumer Information to Others*
Individual-Level, *including:* Financial and Credit Data; Lifestyle, Hobbies, Interests, and Activities; *Demographics*	**Potential Privacy Threats**		
	* Appropriation: - Little, or no, input over whether, and how, information is used. * False Light: - Misclassification	* Appropriation: - Little, or no, input over whether, and how, information is used. * Intrusion: - Misdirected or inappropriate advertising. - Loss of "right to be left alone"	* Appropriation: - Little, or no, control over information dissemination. - Little, or no, control over how information is used. * Disclosure: - Public disclosure of erroneous or potentially embarrassing private facts. * Intrusion: - Misdirected or inappropriate advertising. - Loss of "right to be left alone"
Group-Level, including: Inferred Lifestyle, Hobbies, Interests, and Activities; Inferred Values and Attitudes; Geodemographic Categorizations; Broad Demographic Categorizations; Broad Geographic Categorizations	**Potential Privacy Threats**		
	* False Light: - Misclassification	* Intrusion: - Misdirected or inappropriate advertising. - Loss of "right to be left alone"	* Appropriation: - Little, or no, control over information dissemination. - Little, or no, control over how information is used. * Disclosure: - Public disclosure of erroneous or potentially embarrassing private facts. * Intrusion: - Misdirected or inappropriate advertising. - Loss of "right to be left alone"

FIGURE 2
Direct Marketers' Information Use Practices and Consumer Privacy

nign in that survey data provide the basis for dividing a market into clusters of similarly behaving consumers. False-light concerns are precluded by the generalized nature of the projections, while the voluntary nature of the data collection effectively eliminates appropriation concerns. Furthermore, even if a misclassification were directly associated with a specific consumer, and that information were subsequently disseminated to others, the primary (and in many cases, only) "harm" from a legal or social perspective would be the reception of misdirected advertising (60). Similarly, the use of generalized or group-level data, erroneous or otherwise, to guide message or media strategies undoubtedly results in many consumers receiving more advertising, or possibly more irrelevant advertising, than they desire (i.e., intrusion). In any case, consumers can easily alleviate the harm by discarding or ignoring the offending message.

In actuality, intrusion, disclosure, and appropriation are actionable privacy concerns only when the direct marketing practices involve, and adversely affect, specific identifiable consumers. Even this, however, represents a necessary, but not sufficient

condition with respect to privacy. In other words, market segmentation and profiling, media planning, or message design often use individual-specific information, but rarely, if ever, infringe upon consumer privacy in such a way as to cause significant personal harm. Thus, although all four of Prosser's privacy torts are relatively easily applied (see Figure 2), the lack of significant tangible harm greatly reduces their relevance (3, 60). For example, not allowing individual consumers to have input into how marketers use data about them to segment markets, choose media, or design messages, likely results in much misclassification or misdirected advertising, but little legal basis for invasion of privacy claims. The legal applicability of intrusion is limited by the benign nature of the intrusion (i.e., advertising such as direct mail or a telemarketing phone call) as well as the availability of easily implemented solutions (e.g., discarding the advertising or hanging up on the caller). Similarly, the "highly offensive and objectionable to a person of ordinary sensibilities" standard virtually eliminates the applicability of the disclosure dimension when it comes to marketing information practices.

In fact, it appears that in the direct marketing domain, any attempts to invoke privacy claims must center around appropriation arguments. As noted, marketers have operated under the assumption that they can do what they want with individual-level information, especially that which consumers have knowingly and willingly provided. Thanks to the advent of relational databases (36), the increased use of direct response and database marketing tactics (19), and the relatively indiscriminate selling and renting of personal information collected in the course of marketing exchanges, this may no longer be an appropriate assumption. From the perspective of many consumers, using large amounts of specific personal details and trading that information to others represents an unwarranted appropriation and exploitation. As technology expands marketers' data manipulation techniques even further, statistical representations will likely disclose more about individuals than physical representations. And if an individual legally has some control over the ways their physical likeness can be used, it logically follows they should have some control over the ways detailed statistical representations are used, particularly when there is a high likelihood that such portrayals are inaccurate, incomplete, or out of date. At the very least, appropriation could be used to buttress the arguments of those, such as Rothfeder (57), who suggested that consumers should be compensated (e.g., paid a royalty) each time their name and specific information about them is disseminated by entities who financially profit from doing so or by entities who have incidentally obtained such data without consumers' knowledge or permission.

CONCLUSIONS

Suggestions and Tactics for Addressing Privacy Issues

In lieu of a widely accepted and agreed upon definition of privacy, consumers, direct marketers, and policy makers are unlikely to come to complete agreement on the answer to the question: When does privacy matter? It is clear, however, that an attempt to answer that question is essential if a framework that balances consumer privacy concerns with the information needs of marketers is to be developed. Figure 3 illustrates an attempt to identify when privacy matters. It also includes specific suggestions that, if implemented, would reduce consumer privacy concerns while still allowing marketers the use of individual-level information. Before getting to the specific suggestions, however, a brief discussion of consumer concerns related to information knowledge and control is necessary.

As the analysis conducted in this article illustrates, when it comes to consumer information, privacy's legal relevance is essentially limited to practices involving individual-specific rather than group-level or generalized data. Understanding the legal basis is important, however, consumer concerns regarding privacy and direct marketers' information practices are not restricted by legal constraints. The legal basis for the use of consumer information is often of little consequence to consumers with gut-level negative reactions to feelings of ignorance (e.g., How did this company get my name?) and loss of control (e.g., I can't control who obtains the information or for what purposes the information is used). Ignoring consumer privacy concerns, or any concern for that matter, is a dangerous business strategy. Recognizing this, the analysis suggests that

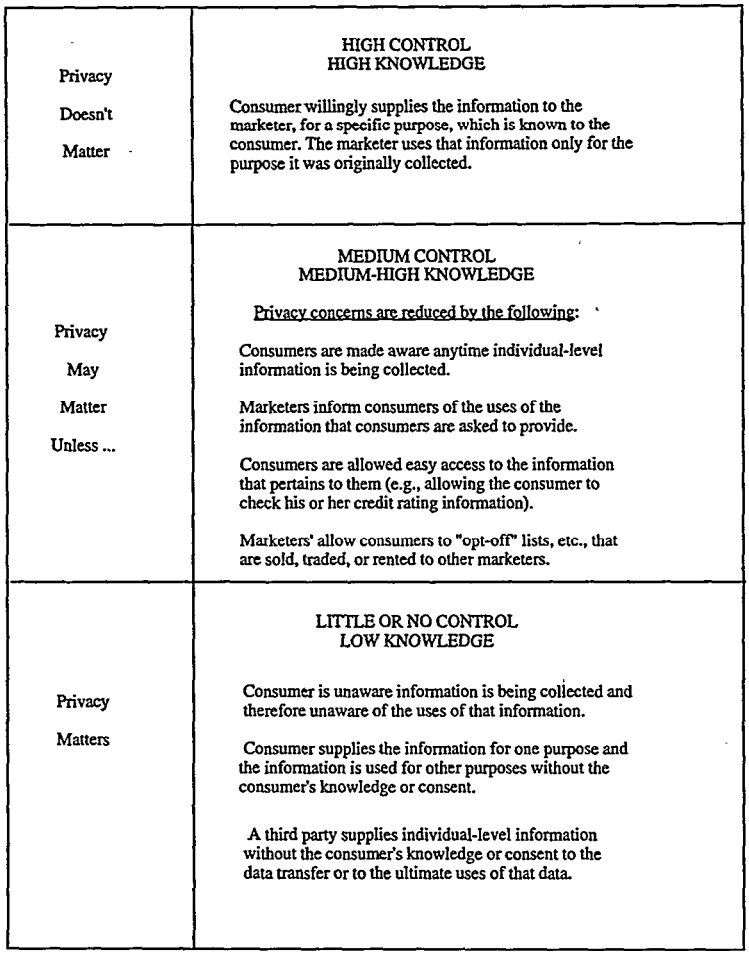

FIGURE 3
Using Amount of Information-Related Knowledge and Control

direct marketers, as a matter of practice, if not of law, should take consumers' knowledge and influence into account when using individual-specific information. Figure 3 illustrates that increasing consumers' information knowledge and control considerably reduce privacy's significance.

More specifically, direct marketers should routinely inform consumers when individual-specific information is collected, let them know how the information will be used, and tell them who will have access to the data. Other visible steps, such as implementing periodic consumer reviews, also would benefit both parties. Consumers' appropriation, disclosure, and false light concerns would be diminished, while the accuracy and currency of marketers' databases would be enhanced. Direct marketers could further alleviate privacy concerns by allowing consumers to opt off lists that are rented to other marketers. Ideally, they would offer consumers a blanket approach (i.e., removing their names from all lists that are rented to others) as well as a selective option (i.e., allowing consumers to indicate the types of companies to which their names could be rented). Notably, the Direct Marketing Association (DMA) has already (Summer 1993) conducted a single-city field test of a selective

opt-off program (29). At worse, such consumer empowerment would greatly reduce appropriation concerns and at best, it would significantly reduce unwanted advertising intrusions.

Implementing the suggestions outlined previously will have a greater impact if direct marketers successfully promote their proactive efforts to consumers and policy makers. Consumers and policy makers must be made aware of industry efforts to lessen consumer concerns. In addition, direct marketers' consumer education efforts need to emphasize that striking a balance between marketers' information needs and consumers' privacy concerns necessitates compromises. Consumers and policy makers must be reminded that privacy issues and concerns cannot be considered in a vacuum, and even in the commercial world, privacy clashes with freedom of speech. Direct marketers, in the course of carrying out promotional campaigns, rely on consumer information to select audiences, media, and messages. Restrictions on the gathering and use of individual-specific information would restrain the free flow of ideas in the commercial marketplace (50-52). This not only implies that measures designed to increase consumers' privacy may come at the expense of direct marketers' rights, it suggests such benefits will carry some consumer costs (60). For example, reducing direct marketers' ability to gather and use individual-specific information may alleviate disclosure and false light concerns, but also will likely increase reliance on mass advertising and thereby exacerbate intrusion concerns. Regulators, legislators, and consumers thus need to recognize that reduced advertising clutter, more relevant advertising messages, and reduced marketing costs are tangible and quite significant benefits that arise when direct marketers use individual-level information. Conversely, direct marketers need to recognize that not only is consumers' ability to protect or limit the use of individual-specific information directly related to the extent they are aware of information gathering and use practices, so also is their ability to judge the appropriateness of privacy measures.

Finally, since laws and regulations have produced more symbolic than real privacy protection, professional and industry self-regulation needs to play an integral role in alleviating consumer doubts and concerns (18, 47). Arguing that industry self-regulation is the best option for consumers is not a popular position in some circles. According to Jones (30:145), the industry "has not been conspicuous by its ability to resolve the problems that give rise to demands for enforceable government performance standards." Jones suggested a mix of both mandatory and voluntary regulation with voluntary codes taking the leadership in such sensitive areas as database sharing and matching and the compilation and dissemination of narrowly categorized mailing lists. Mandatory regulations may be necessary. However, more time should be allotted to industry self-regulatory efforts before governmental regulations are mandated. Even though it is seldom perfect, self-regulation as a form of private interest government provides an effective form of societal control over marketing behavior (8). As the suggestions provided in this section illustrate, the possibilities for self-regulation with respect to information practices are significant. Consumer privacy, as it relates to direct marketing practices, is still a somewhat nebulous concept. It is hoped that this article has provided a clearer understanding of privacy and how it relates to direct marketers' information practices. This is an important step because, as is true in any situation, the problem must be clearly defined before potential solutions can be developed. Knowing when privacy matters is also essential when evaluating the usefulness of solutions/suggestions for reducing consumer privacy concerns.

Suggestions for Future Research

Regardless of whether industry or government takes the lead in resolving these issues, the academic community must become actively involved in efforts to define and promote professional and ethical standards relating to the use of individual-specific consumer information. At a scholarly level, there is a dire need for theoretical frameworks that expand the concepts discussed here as well as for further research on the ways privacy issues impact marketers and consumers. Important questions, dealing with the nature of consumers' privacy concerns and consumers' knowledge of direct marketers' information practices remain unanswered. For instance, an examination of consumer reactions to marketers' specific information practices is required to develop

a better understanding of consumer privacy concerns. The identification of the specific information practices that cause the greatest consumer concern would be of tremendous value in developing strategies to lessen consumer concerns. Furthermore, issues relating to the effects of privacy concerns on attitudes toward direct marketing, and the relationships between privacy and advertising annoyance, have yet to be examined. ■

REFERENCES

1. Alberta, Paul M. (1993), "Large Majority of Consumers Worry About Privacy: New Harris Survey," *Direct Marketing News* October 4, 8, 44.

2. Aldrich, Robert (1982), "Privacy Protection Law in the U.S.," *National Telecommunications and Information Agency Report*, Washington, DC: U.S. Department of Commerce.

3. Awerdick, John H. (1992), "Reflections on Privacy: Looking for Meaningful Distinctions in a Regulated World," *Advents Marketing*, 32(5), 1-4.

4. Ballinger, J. (1991), "Privacy Called the Top Direct Marketing Threat; USPS, Environment Tie for Second," *Direct Marketing News* (August 26), 3.

5. Bigelow, Robert P. (1986), "Computers and Privacy: An American Perspective," *Information Age*, 8(3), 134-140.

6. Bird, Laura (1990), "Marketing in Big Brother's Shadow," *Adweek's Marketing Week* (December 10), 26-28.

7. Block, Martin P. and Brezen, T. S. (1990), "A New Technique of Media Planning: Using Databases to Segment General Media Audiences, "*Journal of Media Planning* 5(l), 1-14.

8. Boddewyn, J. J. (1989), "Advertising Self-Regulation: True Purpose and Limits," *Journal of Advertising* 18(2), 19-27.

9. Carnevale, Mary Lu, and Lopez, Julie A. (1989), "Making a Phone Call Might Mean Telling the World About You," *Wall Street Journal* (November 28) A1, A8.

10. Cook, William A. (1991), "Information Technology Batters Down Ancient Walls," *Journal of Advertising Research*, 31(4), 7-8.

11. Crawford, Rick (1994), "Techno Prisoners," *Adbusters*, 3(2), 16-23.

12. Culnan, Mary (1995), "Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing," *Journal of Direct Marketing*, 9(2), in press.

13. Dickler, Gerald (1936), "The Right of Privacy: A Proposed Redefinition," St. Louis University Law Journal, 70, 425-441.

14. *DMA Report on Privacy* (1992), New York: The Direct Marketing Association, Inc.

15. *Equifax Report on Consumers in the Information Age*, (1990), Atlanta: Equifax.

16. Freedman, Warren (1987), The *Right of Privacy in the Information Age*, *New* York: Quorum Books.

17. Foxman, Ellen R. and Kilcoyne, Paula (1993), "Information Technology, Marketing Practice, and Consumer Privacy: Ethical *Issues*, "*Journal of Public Policy & Marketing* 12(1), 106-119.

18. Gandy, Oscar and Simmons, C. E. (1986), "Technology, Privacy and the Democratic Process," *Critical Studies in Mass Communication*, 3(2), 155-168.

19. Goldman, Debra (1991), "Census an Advertiser's Dream, But Database Motherlode Poses Ethical Problems," *Adweek*, 12(15), 1, 4.

20. Goodwin, Cathy (1991), "Privacy: Recognition of a Consumer Right," *Journal of Public Policy & Marketing* 10(1), 149-166.

21. Gray, Peter J. (1990), "Federal Privacy Legislation," *Credit World*, 78(4), 18-22.

22. Griswold et al. *v.* Connecticut (1965), 381 U.S. 479; 85 S. Ct. 1678; 1965 U.S. Lexis 2282; 14 L. (Ed. 2d 510).

23. Gross, Hyman (1964), *Privacy– Its Legal Protection*, Dobbs Ferry, NY: Oceana Publications.

24. *Harris-Equifax Consumer Privacy Survey* (1991) Atlanta: Equifax.

25. *Harris-Equifax Consumer Privacy Survey* (1992), Atlanta: Equifax.

26. *Harris-Equifax Health Information Privacy Survey* (1993), Atlanta: Equifax.

27. Hume, Scott (1991), "Consumers Target Ire at Data Bases," *Advertising Age* (May 6) 1.

28. Husted, Bill (1991), "Companies Already Have Profiles of Callers," *Atlanta Journal* (March 24), A1, A4.

29. Jaffee, Larry (1993), "DMA to Conduct Test This Summer of 'Selective Opt-Out Program," *Direct Marketing News*, 15(25), 3.

30. Jones, Mary Gardiner (1991), "Privacy: A Significant Marketing Issue for the 1990s," *Journal of Public Policy & Marketing*, 10(1), 133-148.

31. Katz, James E. (1988), "U.S. Telecommunications Privacy Policy: Socio-Political Responses to Technological Advances," *Telecommunications Policy*, 12(4), 353-368.

32. Katz, James E. and Tassone, A. (1990), "The Polls: Public Opinion Trends, Privacy and Information Technology," *Public Opinion Quarterly*, 54, 125-143.

33. Katz *v.* United States, U.S. 389, (1976).

34. Lacayo, Richard (1991), "Nowhere to Hide," *Time* (November 11). 34-40.

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

36. Laurie, S. (1990), "We Know Everything About You," *The Banker* (November), 90-91.

37. Levin, Gary (1991), "Databases Loom Large for the '90s," *Advertising Age* (October 21), 22-24.

38. Light, Larry (1990), "The Changing Advertising World," *Journal of Advertising Research*,30 (February/March), 30-35.

39. Litle, Thomas (1992), "The Great Database Debate 1992: Who Owns the Data?" Paper presented at the 75th Annual Conference and Exhibition of the Direct Marketing Association, Dallas, October 25-28.

40. McCarthy, J. Thomas (1990), *The Rights of Publicity and Privacy*, New York: Clark Boardman.

41. McCrohan, Kevin F. (1989), "Information Technology, Privacy, and the Public Good," *Journal of Public Policy & Marketing*, 8, 265-278.

42. McIllhenry, James H. (1990), "The New Consumerism: How Will Business Respond?' in *Up With Consumers*, Direct Selling Educational Foundation, 10, 5.

43. McWhirter, Darien A. and Bible, Jon D. (1992), *Privacy as a Constitutional Right: Sex, Drugs, and the Right to Life*, New York: Quorum Books.

44. Miller, Cyndee (1995), "Concern Raised Over Privacy on Infohighway," *Marketing News*, 29(1), 1, 7, 11.

45. Miller, Michael (1991), "When a 'Junker' Calls, This Man is Ready for Revenge," *Wall Street Journal* (June 24), A1 A4.

46. Milne, George R. and Gordon, Mary Ellen (1993), "Direct Mail Privacy-Efficiency Trade-offs Within an Implied Social Contract Framework," *Journal of Public Policy & Marketing*,12(2), 206-215.

47. Nowak, Glen J. and Phelps, Joseph (1991), "Quenching the Thirst for Personal Information: Advertising Practices versus Consumer Privacy." Paper presented at the Association for Education in Journalism and Mass Communication Annual Convention, Boston, August 9-13.

48. Nowak, Glen J. and Phelps, Joseph (1992), "Understanding Privacy Concerns," *Journal of Direct Marketing*,6(4), 28-39.

49. Plesser, R. L. and Cividanes, E. W. (1991), *Privacy Protection in the U.S.: 1991 Survey of Laws and Regulations Affecting Privacy in the Public and Private Sector*, Washington DC: Direct Marketing Association, Consumer Affairs Department.

50. Posch, Robert (1987), "How the Law(s) of Privacy Impact Your Business," *Direct Marketing* 50(0ctober), 74-82, 99-102.

51. Posch, Robert (1988), "Do We Have Constitutionally Protected Access to Our Customers," *Direct Marketing*, 51(June), 92-95.

52. Posch, Robert (1989), "Can We Have a la Carte Constitutional Rights," *Direct Marketing*, 52(July), 76-77.

53. Prosser, William (1960), "The Torts of Privacy," *California Law Review*, 383(48), 392-398.

54. Rapp, Stan and Collins, Tom (1990), *The Great Marketing Turnaround: The Age of the Individual and How to Profit from It*, Englewood Cliffs, NJ: Prentice-Hall.

55. Regan, Priscilla M. (1988), "From Paper Dossiers to Electronic Dossiers: Gaps in the Privacy Act of 1974," *Office Technology and People*,3, 279-296.

56. Rotenburg, Marc (1993), "Communications Privacy: Implications for Network Design," *Communications of the ACM*,36(8), 61-68.

57. Rothfeder, Jeffrey (1992), *Privacy for Sale: How Computerization has made Everyone's Private Life an Open Secret*, New York: Simon Schuster.

58. Salvaggio, J. L. (1989), "Is Privacy Possible in an Information Society," in *The Information Society: Economic, Social and Structural Issues*, J. L. Salvaggio, ed., Hillsdale, NJ: Erlbaum, pp. 115-130.

59. Shepard and Associates (1990), *The New Direct Marketing*, Homewood, IL: Business One Irwin.

60. Sherman, Robert L. (1991), "Rethinking Privacy Issues," *Direct Marketing*, 53(12), 40-44.

61. Stone, E. F. and Stone, D. L. (1979), "Information Privacy: A Bibliography with Key Word and Author Indices," Unpublished manuscript, Purdue University, Information Privacy Research Center.

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

63. Toth, Victor J. (1990), "Calling Line ID vs. Privacy: A Regulatory Update," *Business Communication Review*, 20(3), 62-66.

64. Tuerkheimer, Frank M. (1993), "The Underpinnings of Privacy Protection," *Communications of the ACM*,36(8), 69-73.

65. Turn, Rein (1985), "Privacy Protection," *Annual Review of Information Science and Technology*,20, 27-50.

66. *U.S.A. Today* (1995), "Lawsuit Over Credit Errors Gets Go-Ahead" (January 20), 1A.

67. Wang, Paul and Petrison, Lisa A. (1993), "Direct Marketing Activities and Personal Privacy," *Journal of Direct Marketing*, 7(1), 7-19.

68. Westin, Alan J. (1967), *Privacy and Freedom*, *New* York: Atheneum.

69. Zacchini *v.* Scripps-Howard Broadcasting Co. (1977), 433 U.S. 562; 97 S. Ct. 2849; 1977 Lexis 145; 53 L. Ed. 2d 965; 40 Rad. Reg. 2d (P & F) 1485; 5 Ohio Op. 3d 215; 2 Media L. Rep. 2089; 205 U.S.P.Q. (BNA) 741.