Personal Information Privacy Issues Relating to Consumption in the U.S. Marketplace

Information exchange is a two-edged sword, producing both consumer benefit and threat to personal privacy. Consumers, regulators, and firms will continue to struggle with the meaning of personal privacy in the information age until clear definitions are set, monitoring and enforcement rules put in place and tried in courts. A Consumer Personal Information Flow Cycle (CPIFC) is introduced to map diverse categorical areas of personal information disclosure, storage and manipulation of the personal data and the integration of varied databases. The Consumer Personal Information Flow Cycle provides a beginning framework for capturing the scope of personal privacy information and the processes by which information is traded. The cycle is used to identify points where privacy may be violated, where research is needed, where regulation and monitoring might be effective and where educational intervention is appropriate.

Marjorie I. Bonavia, Ithaca College[1]
Lois Wright Morton, Cornell University[2]

Introduction

The electronic dossier, which is available to anyone with access to the Internet, is only one of the many potential sources of privacy invasion. In this paper, information privacy is defined as it relates to consumers. Next, three types of threats to personal privacy are identified. Lastly, a Consumer Personal Information Flow Cycle (CPIFC) is proposed to map a) categorical areas of personal information that individuals give away during activities of daily life, b) information storage and manipulation, and c) integration of varied databases.

Defining Privacy

Personal privacy has concerned American citizens long before the 1990's Information Age and the U.S. Office of Consumer Affairs declared it a major 1997 agenda item (Equifax-Harris Consumer Privacy Survey, 1996). The debate surrounding the exact definition(s) of personal privacy can be traced back to legal scholars Samuel D. Warren and Louis D. Brandeis (later a Supreme Court Justice) (Larson, 1992). They were the first to define privacy as "the general right to be left alone" in an 1890 Harvard Law Review article (Warren & Brandeis, 1890, p. 193). Brandeis and Warren were among a handful of individuals, before the 1970's, to make comment on something that many speculators of the next congressional election view as a potential hot issue (McLean, 1995).

Traditionally, privacy has been defined by physical things like walls or the distance of a whisper (Dunn, 1997). The U.S. Constitution makes no reference to, and has no clear definition of, privacy as an American right (Larson, 1992). Therefore, the task of defining privacy as it pertains to the individual consumer is not easily accomplished. "Privacy, like an elephant, is more readily recognized than described" (Young, 1978, p. 2). There are many different definitions of privacy that articulate individual interpretations. Philosophers, psychologists, sociologists, journalists, legal scholars, business professionals and consumers attach a different meaning to privacy. However, two common themes emerge from definitions and meanings assigned to privacy: accessibility (Bok, 1982) and control (Smith, 1979; Brandeis, 1890).

With regard to accessibility, Sissela Bok defined privacy as a "condition of being protected from unwanted access by others--either physical access, personal information or attention" (1982, p. 11). Access has to do with aspects of consumption which directly apply to such practices by marketers as observing consumers' purchasing behaviors and recording of brands purchased. Accessibility, however, is only part of the privacy issue.

Robert Ellis Smith's definition of privacy emphasizes the other common theme, control. "Privacy is the right to control information about yourself, as in the right to prevent disclosure of private facts or the right to know which information is kept on you and how it is used" (1979, p.323). Control-based definitions are more comprehensive than access-based definitions but may not be useful for policy (law or business) because they are too broad. In fact, the idea of privacy being a right in a computerized, free market is a difficult position to argue. Consider this: Over "111 million Americans rely upon the convenience and diversity of products when shopping by

phone or mail" (United States Department of Commerce, 1995, p. 20). Consumers who are attracted to this type of shopping, business argues, give tacit support to practices such as profiling (collecting personal information on specific households from many different sources to predict propensity to purchase certain products) which help make it easier to find consumers who would be interested in unusual assortments typical of mail order.

What is needed is a definition of privacy that combines aspects of both access and control. The definition should cover the many acts defined as consumption and make clear the type of control (direct or indirect) and at what point (before, after, during a transaction) control should be monitored and regulated. It is not the goal of this discussion to put forth a specific definition, but rather to reveal a void in the field of consumer research for a definition of privacy.

For this paper, "information privacy" includes consumers' need to have access to their information protected and to be able to control personal information (United States Department of Commerce, 1995). Personal information is based on three sources: "public records; internal records--records collected directly from the individual by the profiler; and external records--records obtained by the profiler not directly from the individual but from some third party" (p. A-3). Information privacy is "an individual's claim to control the terms under which personal information (information that can be linked to an individual or household) is acquired, disclosed, and used" (p. 7-8).

Threats to Personal Privacy

On the surface, the collection of personal information by institutions in particular settings may seem innocuous. Institutions have specific purposes behind assembling these data bases. These purposes include existing product revision and testing, new product development, and niche marketing. Part of the cost to consumers, when they purchase a good or service, is the sacrifice of personal information which can lead to the invasion of their privacy (MacNeil, 1992). The unspoken, but normative, expectation is that personal information, disclosed through acquisitional transactions, will mutually benefit the consumer and the institution. In many instances, the use of credit cards as a payment mechanism produces automatic behavior on the part of the consumer. As a result, consumers, particularly in routine purchases, may not evaluate the type or extent of information provided and the benefit or detriment that could occur to them.

The relationship of information disclosure by consumers and acquisition by institutions necessitates a closer examination of potential privacy threats. Three major threats to privacy occur in information transactions. First, the individual loses control when personal information is shared. Second, when extraneous data is obtained (data not necessary to the transaction), data surplus is generated. Third, personal information, once acquired, is the property of the institution to store, manipulate, and sell without consumer knowledge or consent.

The first threat to privacy, loss of control, results from the "mere awareness" that strangers may have of certain types of information. Loss of control is more than just other people knowing individual salary range, age, telephone number, and the number of kids in the family. Information may include physical or mental ailments that could cause embarrassment, injury to personal ego, social harassment or employment discrimination (United States Department of Commerce, 1995). This information might also include criminal convictions, divorce settlements, lottery winnings, medications taken, and sexual preferences.

The second threat to privacy occurs when institutions obtain more personal information than they need to meet consumer expectations. For example, a mail order catalog will need a credit card number to bill and a telephone number to reach the consumer should they have questions about the order, but they do not need a bank account number. Similarly, a local store may invoke certain price savings if a consumer furnishes a name, address, and social security number. The name and address are necessary to identify the consumer for future savings. The disclosure of a social security number denotes no direct benefit to the consumer yet to firms interested in creating consumer databases the social security number is the only unique consumer characteristic. Both the bank account number and the social security number are extraneous to their particular transaction. The institution has generated surplus information that can be traded to other institutions.

The third threat to privacy is the manipulation and transfer of personal information to other institutions which may use it "improperly, unfairly or for purposes other than those intended by the individual" (United States Department of Commerce, 1995, p.3). For example, a security number given as extraneous information in the previous example can be used by the institution to make more sellable the original data given. This violates the concept of mutual benefit in the acquisition transaction because it is the use of data beyond the original purpose. Improper usage of personal information data, for purposes not originally intended, brings into focus issues of storage, manipulation, integration and ethical transfer.

Consumer Personal Information Flow Cycle

The Consumer Personal Information Flow Cycle (Figure 1) captures the relationships between consumers and institutions and among institutions as information is exchanged. The cycle consists of three levels of information exchange and processing plus feedback recirculation. The first level, consumer settings and activities, triggers the information exchange process. In the second level institutions store and manipulate personal information data for their own uses. The third level, integration, combines the institutional buying and selling of personal information data and integrates the obtained data into their own data bases. Although threats to privacy can occur at all three levels, the third level, integration (the trading of data to create new sets) is the newest and most controversial.

The Consumer Personal Information Flow Cycle begins with ten major categories of daily life activities that require pieces of personal information from consumers. These data bits are stored in a form that can be linked back to an individual's identity. The first level, consumer settings and activities, represents areas of disclosure of personal information (by consumers) and its acquisition (by institutions). When institutions ask consumers to reveal personal information, it is with a specific intent and purpose. For example, the bank request for salary and current debt load assists in determining how much debt a person can handle when applying for a loan. Accurate information is essential in keeping the costs of credit low for consumers overall. The settings and activities shown at level one often require consumers to disclose personal information in order to complete the transaction (i.e., to gain access to a product (loan) or exercise citizenship (voter registration)). The nature of some of these transactions actually deem the disclosure of information itself as payment for a product sought by a consumer. For example, a supermarket shopping discount card gives cents off products or free products for the cost of consumer personal information that is given each time the consumer swipes their card and allows the retailer's database to collect the brands they prefer. The same transaction occurs when citizens give their name, address and birth date for the right to vote in a government election.

The second level of the Consumer Personal Information Flow Cycle represents the storage and manipulation processes which occur after personal information is disclosed and acquired. This level utilizes sophisticated technologies and information management systems to inform the institution about the characteristics of their consumers. Information privacy is not violated at the storage point if personal information has been used for purposes originally stated or it is combined with other consumer information to present aggregate information. The dotted lines between institutions indicate the incompleteness of firm information and the desirability, from the firm perspective, of obtaining additional information from other firms.

In data manipulation, statistical techniques are employed to develop models of consumers (Pride & Ferrell, 1997). These models assist firms in their analyses of what, how, when, how much, and how often particular products are used/purchased/solicited. A compilation of buying characteristics with such personal information, as name and address, represent a consumer profile. When there is a lack of personal information needed for the statistical model to be computed, then the institution may seek the information by asking the consumer directly, or the institution may seek it in another, outside (secondary) database. The cost of directly asking consumers for the information in terms of trust and actual dollars usually discourages the direct acquisition approach. Moreover, institutions may want to learn details that a consumer may not wish to reveal such as age, race, religion, and sexual orientation (Larson, 1992). As institutions seek to enrich their own databases to improve the accuracy of consumer profiles, secondary sources become a viable and cheap solution.

When institutions seek enrichment of data from outside sources, the third level, integration, is activated. This is where the exchange of data sets and access to public information through the Freedom of Information Act are combined to create new data bases. In the transition from the second level of storage and manipulation to the integration level, value in dollars is placed on data. Information becomes a commodity that is traded, bought, and sold in a $3 billion per year market (United States Department of Commerce, 1995, p. 3). Institutions may choose from over a thousand commercial databases for secondary information (Piller, 1993). Occupations like list compiler, profiler and list broker are common. Technology methods, such as matching and enrichment, are examples of the efficiencies that can be achieved in database profiling for better consumer targeting. Matching is done when personal information contained in individual records are given codes that identify the type of information. Name, address, social security number and frequency of purchase are just a few examples of information that is coded. The advantage of coding is two-fold. When integrating databases, duplicate names and addresses can be eliminated. This saves money and eliminates consumer frustration over duplicate mailings (Stone, 1996). The integration of original and secondary databases at great speed is also advantageous, creating economies of scale for large commercial databases like Donnelly Marketing, Inc. Among the most efficient, Donnelley boasts over 150 million individuals in their database (United States Department of Commerce).

Enrichment of data involves two databases. Enrichment is what occurs after two separate databases have been matched. The addition of information (demographing and psychographing) beyond a name and address will add to an institution's understanding of its consumers. "In essence [enrichment of] a database lets you learn more about your customers and why they buy so you can nurture your relationship with them for many profitable years" (Stone, 1996, pp. 187-188). Large storage capacity and greater computing capabilities have improved institutional capacity to integrate data received originally from consumers with data bought from outside the institution.

It is at level three, when the information is traded, that it "turns an ethical corner." The personal information that was acquired and disclosed for one purpose can be used for purposes other than originally intended. When internal databases, as shown in the model, are expanded to include personal information from public (government) and private (commercial) sources, both institutions--the one selling or trading the data and the one receiving the data--may violate proper usage in the information privacy definition. For example, data given by consumers that was originally intended to qualify them for a drivers license or I.D. card, containing what type of car driven, insurance carrier, convictions for a felony or DWI, etc., can be sold for direct marketing purposes in the majority of states (Larson, 1992).

After enrichment, matching and profiling are complete, the new data base can be used to reconnect with consumers in a new way, creating a feedback loop from the firm or institution to the consumer. The firm now has a better idea of who their target market is from the integration of secondary databases and statistical modeling. It can then respond to this new information by improving existing products or creating new ones to better satisfy consumer needs and desires. The institution may also improve the quality of targeting consumers that may be interested in their products, improving the effectiveness of direct mail, telephone and computer solicitations.

When integration is effective and well-received by consumers, convenience, rather than privacy violation, occurs. The right product has reached an interested consumer. Sometimes, integration is successful but the offer itself is untimely and the consumer "trashes" the product offer. When integration has erred by the usage of old data (you are now married) or incorrect data (misspelled names), the profile is statistically incorrect (a vegetarian receives offers for steaks by mail), and the consumer may feel threatened, frightened, violated, insulted, angry or simply annoyed. In some instances, the consumer will react aggressively by contacting the Federal Trade Commission, the Direct Market Association, or a private association to have their name removed from secondary use altogether. The 1996 Consumer Privacy Survey by Equifax-Harris recorded a four-point increase in concern of personal privacy issues (Equifax-Harris Consumer Privacy Survey 1996).

The boundaries of privacy have been altered by market competition for consumers and by computer technologies. Information exchange is a two-edged sword, producing both consumer benefit and a threat to personal privacy. Integrated information may be accurate, but considered an invasion of personal privacy. If the Internal Revenue Service integrates all data, will citizens think of this as a convenience or as surveillance? Consumers, regulators, educators and firms will continue to struggle with the meaning of personal privacy in the information age until clear definitions are set, and monitoring and enforcement rules are put in place and tried in courts. Integration is a complicated concept for consumers to grasp. The Consumer Personal Information Flow Cycle provides a beginning framework for consumer educators, businesses, policymakers, and regulators to develop appropriate education and business practices. Many institutions think that silence among consumers is tacit support for information gathering and integration practices. Without additional research, it is impossible to know the extent to which consumer privacy is being violated. A compilation of flagrant abuse of information is a first step toward finding common ground for delineating privacy issues. Deeper understandings of how third party information exchange affects individuals and where society wants to draw the line on privacy definitions are necessary for appropriate education and regulatory interventions to be put in place.

References

Bok, S. (1982). Secrets. New York:Pantheon.

Bernstein, N. (1997, September 15). High-tech sleuths find private facts online. (Cybertimes, Http://www.nytimes.com).

Credit card holders, banks and privacy. (1996, March/April). Privacy and American Business,4, pp 7,17.

Equifax-Harris. (1996). Consumer privacy survey. (Study 638114). New York:Louis Harris and Associates.

Harris-Equifax. (1996). Health information privacy survey. (Study 934009). New York: Louis Harris and Associates.

Larson, E. (1992) The naked consumer. New York: Henry Holt and Company.

MacNeil, H. (1992). Without consent: The ethics of disclosing personal information in public archives. Metuchen, N.J.:The Scarecrow Press, Inc.

McLean, D. (1995). Privacy and its invasion. Westport, C:Praeger.

Piller, C. (1993, July). Privacy in peril. MacWorld, p. 8.

Pride, W. & Ferrell, O.C. (1997). Marketing concepts and strategies (10th ed.).:Houghton Mifflin.

Privacy Rights Clearinghouse. (1995, January). Fact sheet. Privacy survival guide: How to take control of your personal information. (No.1). pp 1-4.

Smith, R.E. (1979). Privacy. G.C. New York:Archer/Doubleday.

Stone, B. (1996) Successful direct marketing methods. Lincolnwood, IL:NTC Business Books.

Survey trends underpin rising Washington privacy activity. (1997, Special Issue). Privacy and American Business. 3, pp. 1-3, 6-7, 14.

United States Department of Commerce. (1995). Privacy and the NII: Safeguarding telecommunications-related personal information. (1st ed.). Washington, DC:U.S. Government Printing Office.

Warren, S.D. & Brandeis, L.D. (1890). The right to privacy. Harvard Law Review, p. 193.

Wartzman, R. (1994, December 23). Information, please: A research company got consumer data from voting rolls. Wall Street Journal, p. 1.

Young, J.B. (1978). Privacy. New York:Wiley.

Endnote

1. Instructor of Marketing
2. Senior Extension Associate in Policy Analysis and Management