Information & Ethics in INSURANCE

by Daniel J. Brown, Linda Gammill, Norma L. Nielson, and Mary Alice Seville

Abstract

Insurance companies have a right to gather information about persons who wish to apply for insurance. That right has to be balanced by the applicant's right to privacy. Insurance companies abuse personal information at their own and the industry's risk. This article summarizes the issues involved and makes some recommendations to help the insurance industry avoid regulation of information gathering and use.

Guidelines for Information Gathering

> "I used to think that credit reporting services posed the greatest threat to direct marketing as we know it. Because of the massive snooping and record collection of our personal financial records . . . I thought that the resultant consumer backlash would reach Congress and we would be legislated out of business.
>
> I was wrong. The credit reporting crowd is a pussycat compared to the insurance and drug industries." [Hatch, 1993, p. 8]

Very few, if any, rights in society are absolute. Where the interests of two parties conflict, they must be weighed against each other and one right must be given precedence over the other. Insurance companies have a right to gather information about persons who wish to apply for insurance. This is essential to determine the risk classification of the applicant. Without this information insurance companies would have no basis to determine whether the person is insurable and, if so, at what price. The benefits are not limited to the insurance company, however. Other persons insured by the company are able to enjoy lower insurance rates as a result of accurate risk classifications. By accurately predicting insurance claims, insurance companies are able to offer their services without adding an exorbitant risk premium to the expected losses. Risk classification also allows differential pricing, whereby persons who are lower risks are rewarded with lower premiums. Without differential pricing, these people would essentially be penalized by the claims of other higher risk customers. This is an illustration of Rawls' theory of justice. Rawls believed all economic goods and services should be distributed equally except when unequal distribution would benefit society.

According to Nowak and Phelps [1995], insurance information-gathering practices appear to be legitimate with regard to the intrusion, disclosure, and false light elements of Prosser's classic privacy framework. According to Prosser, (1960, p. 389) a defendant would be liable for an invasion of privacy if found guilty of one of the following:

- intrusion upon plaintiff's seclusion or solitude, or into his or her private affairs
- public disclosure of embarrassing private facts about the plaintiff
- publicity that places the plaintiff in a false light in the public eye
- appropriation for the defendant's advantage of the plaintiff's name or likeness.

Two elements serve to reduce the impact of the intrusion element:

1. Consumers knowingly and willingly subject themselves to many forms of data gathering (e.g., TV viewing research). The fact that the findings of such data-gathering experiments are presented at a generalized level further reduces the intrusion element.
2. Actionable privacy issues in the past have tended to be restricted to physical invasions of privacy. In order to constitute an invasion:
    a. The area invaded must have been truly private.
    b. There must have been no valid reason for the intrusion.
    c. The intrusion must have been highly offensive to a reasonable person.

The insurance company's right to information is not unqualified, however. It must be balanced against the applicant's right to privacy. In most instances at present, the individual may only invoke his or her right to privacy in those cases where there has been an invasion of privacy by a government body or official. Where a private body disseminates accurate information about an individual, the individual has no recourse under the law to protect him/herself except in certain limited instances.

Insurance companies abuse personal information at their own and the industry's risk. Law is shaped by the dominant demands in society at any given time. The literature points to a growing consumer activist movement that seeks to place shackles on blatant invasions of privacy being committed with impunity by some private organizations. Farsighted insurance companies that seek to avoid government regulation are paying close attention to the demands of consumers for greater respect of their personal privacy.

The status of privacy protection as it relates to the insurance industry was thoroughly examined in the late 1970s by the Privacy Protection Study Commission (PPSC). The next section (1) summarizes the findings of the PPSC, and (2) briefly discusses the criticisms of the Commission's recommendations and updates that examination of privacy.

Privacy Protection Study Commission

The mandate of the PPSC was to determine whether the Privacy Act of 1974, which applied only to federal agencies, could be extended to include state and local government agencies and organizations within the private sector. The PPSC concluded that although the underlying principles of the Act were sound, the mechanisms contained in the Act for the implementation of these principles were inadequate and too rigid simply to extend the scope of the Act.

The PPSC operated under the framework of three public policy objectives:

1. Minimizing intrusiveness.
2. Maximizing fairness.
3. Maintaining legitimate expectations of confidentiality.

Minimizing intrusiveness means that agencies were only to collect information that was relevant to the goals of their inquiry. The PPSC suggested that control of certain categories of information (e.g., sexual preference and living patterns) were to be handed over to a government organization. That organization would in turn be responsible to determine which agencies would have access to such information based on their motivation for requesting it.

Maximizing fairness means that records were to be kept accurate, up-to-date, and complete. This was recognized as especially important where the information was computerized since there had been a growing trend for this form of information to replace face-to-face interviews.

The fairness objective could be achieved by requiring that agencies follow three steps when seeking information from individuals:

1. The individual had to be given notice of the information-collecting practices of the agency concerned.

Daniel J. Brown is an associate professor of marketing in the College of Business at Oregon State University.

Linda Gammill is an assistant professor of management information systems in the College of Business at Oregon State University.

Norma L. Nielson is professor and chairholder in insurance and risk management in the Faculty of Management at the University of Calgary.

Mary Alice Seville is an associate professor of accounting in the College of Business at Oregon State University.

Editor's Note:
This article is adapted from a report prepared for the Institute for Applied Ethics in Insurance. Copies of the full report can be obtained by contacting Karen Burger, CPCU, CPIW, at (610) 644-2100 x7805.

INSURANCE

"Those drafting the privacy legislation believed that individuals had little idea how easily confidential information gathered on them was compromised by agencies."

2. A specific authorization form had to be obtained from the individual outlining these data collection practices.
3. The Fair Credit Reporting Act would have to be amended to allow individuals access to the information collected on them. The individual also would be allowed to correct any errors contained in such information.

Furthermore, if an agency rejected an application for coverage by an individual, the agency was to disclose its full reasons for rejecting the application. A rejection solely on the basis of rejections by other agencies would not suffice as a valid reason for rejection.

The objective of legitimate expectations of confidentiality is based upon the need for expanded consumer education. Simply stated, those drafting the privacy legislation believed that individuals had little idea how easily confidential information gathered on them was compromised by agencies. Each agency should be under a duty to treat personal information as strictly confidential save for certain specified exceptions. Any violation of this duty of confidentiality would be actionable in a civil claim by the aggrieved individual.

Trends in Record-Keeping

The PPSC found five disturbing trends in personal data record-keeping in the United States:

1. Information was being collected that went beyond the information needs of the organization collecting the information.
2. Information was being gathered solely for the record-keeping needs of the organization and for dissemination to other organizations.
3. The information being required was of an increasingly personal nature.
4. An increasing number of organizations with which the individual had not yet come into contact were becoming sources of information about personal details of the individual. Organizations were increasingly relying on collaboration between themselves to verify the details given to them by individuals.
5. Finally, the PPSC found that neither law nor technology provides the individual with sufficient protection to secure his or her legitimate interest in the records being kept on him or her.

Recommendations by the PPSC

The PPSC concluded its investigations by laying down several recommendations for consideration:

1. The government should set up channels whereby individuals may question the propriety of information that has been collected on them. If the information is found to be improper, the governmental body could then prohibit its further use or future collection.
2. Pretext interviews should be prohibited. An example of a pretext interview would be an interview between the insurance applicant and a representative of the insurance company where the interviewer attempts to gather information on an applicant under the guise of having some other purpose for that interview.
3. Agencies must exercise reasonable care in selecting insurance support organizations.
4. Agencies must have reasonable procedures to ensure the accuracy, completeness, and timeliness of information that has been collected.
5. Agencies should give prospective clients formal notification of information collection policies and sources that will be used for the collection of information.
6. If the insurance company asks another organization for assistance in gathering information, the secondary organization is subject to the limits contained in the notification of point 5 above.
7. Where the information required by an insurance company is not directly related to the eligibility of the applicant for coverage, the insurance company must make this clear to the applicant.
8. Authorization statements by the company to the individual must be more clearly phrased and explained.
9. The applicant has the right to request an interview with the consumer-investigative agency. In this way the individual can give the agency information that it may have sought elsewhere.
10. The individual has the right to see and copy information held on him or her by insurance companies and support organizations.
11. The individual has the right to request the correction of inaccurate insurance records.
12. The same applies to medical records that are inaccurate.
13. Individuals must be given reasons for their rejection by an insurance company.
14. Agencies are prohibited from denying persons coverage based purely on prior rejections by other organizations.

15. Medical information is to be obtained only from medical sources, or the guardian or spouse of the individual, or the individual him/herself.
16. Insurance companies are under a duty to treat personal information concerning individuals as confidential.

Criticisms of the PPSC Recommendations

The findings of the PPSC were presented to an audience of insurance executives and representatives of consumer reporting agencies at the National Conference on Privacy and the Insurance Industry held in 1977.[1] The principal objections to the recommendations concerned the bureaucratic and administrative red tape and the costs involved. The participants expressed their shared belief that the societal benefits provided by insurance would not improve, and might even be harmed, by the recommendations. M. Croydon Johns summarized the anti-regulation sentiments of the insurance industry by stating that, "Good information gathering and handling comes from good management people who want facts and scorn error. That kind of manager lines up every time with Ben Franklin, 'A gentleman doesn't read another gentleman's letter to his wife.' They regard information in their possession as a trust." [Skipper and Weisbart, 1979, p. 99]

Despite the controversial nature of the recommendations made by the PPSC, these recommendations have formed the foundation of privacy legislation since that time and clarify what government regulation of the information-gathering practices of the insurance industry would entail. The insurance industry must police itself with respect to information gathering if it wishes to avoid further regulation.

Recommended Guidelines

This next section summarizes information from sources newer than Skipper and Weisbart [1979] and consolidates the information into four specific guidelines that are likely to be important in avoiding federal regulation.

1. Information relevance. While government oversight of what is or is not relevant may not be desirable, applicants want and have a right to know that a need exists for the information gathered. If an applicant questions what is asked and the company cannot adequately justify it, the information request should be dropped.
2. Information accuracy. Insurance companies need to take particular care that the information gathered is current and accurate. This is important not only for the company gathering the information, but also for other insurance companies that may share the information in its aggregate form. According to Linowes [1992, p. 199], "About 3 million people each year request changes in their credit reports due to wrong or outdated information. When Consumers Union surveyed 161 reports, they found that one-half contained inaccuracies." A credit bureau official in New York City sampled 1,500 reports from Trans Union, Equifax, and TRW Credit Data and found that 43 percent of the reports contained errors. Needless to say, these statistics should raise red flags for any insurance company.

   Erroneous records usually arise from one of five sources:

   - **Inaccuracy**—erroneous information is included in the primary data. The erroneous data are then used by others who have failed to verify accuracy.
   - **Imperfect rationalization**—this occurs when a person is asked a question and only has a fixed, limited set of choices from which to choose a response (e.g., typical survey-type questions). No explanation is then allowed for the answer chosen.
   - **Bias**—this tends to be in favor of concealing unfavorable facts about individuals rather than unfairly prejudicing individuals.
   - **Error**—this refers to clerical or computer errors in handling data.
   - **Incompleteness**—important material is missing from the record. [Carroll, 1991]

   Although the "storage and transmission of inaccurate non-credit-related information is not regulated by any specific statutes" [Bloom et al., 1994, p. 102], in the case of insurance companies, such information may lead to liability through a defamation suit. In order to reduce the risk of liability for inaccurate information, many companies, including American Express, now regularly invite their customers to review and correct their data files and to remove themselves completely from the company's files.
3. Notification of information gathering purposes, techniques, and sources. A theme arising from current privacy legislation is that information gatherers should notify their subjects of the various issues mentioned above. Although many of these

INSURANCE

"Applicants want and have a right to know that a need exists for the information gathered."

disclosures are included on insurance application forms, these often appear in the form of small print and are phrased in a confusing manner. Generally, people will reveal a great deal of information about themselves to businesses that serve their self-interest. If an applicant is given proper notification of the types of information that will be gathered, the sources of that information, and the rationale for gathering it, the applicant is far more likely to volunteer background information that will place the information uncovered by the insurance company in its proper context.

4. Obtaining the prior consent of the applicant. According to Nowak and Phelps [1995, p. 52], "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." This statement reflects the general thought on obtaining the consent of the individual before engaging in a background check on the individual. Linowes [1992, p. 198] takes a very different view of voluntary consent from that of Nowak. He states that, "A person is especially vulnerable when he seeks insurance coverage. The general authorization form he signs when applying for a policy has been characterized as a 'search warrant without due process.'"

In seeking the consent of patients to new, and, therefore, potentially dangerous, forms of treatment, the medical profession has taken a far more narrow approach to voluntary consent. Although this context differs considerably from gathering information on insurance applicants, the underlying principles are sufficiently universal to be beneficial to any insurance firm that prides itself on high-quality customer service.

The National Institutes of Health [1978] have defined informed consent to consist of five general elements:

1. The individual must be advised of the data gathering procedures to be used and of the purpose of the data gathering undertaken.
2. The data subject should also be informed of the anticipated benefits to be gained from the data-gathering project.
3. Any attendant risks to the privacy of the subject that are "reasonably to be expected" must be explained to the individual.
4. The organization responsible for gathering the data must have personnel available to answer any questions concerning the procedures to be used for the gathering, maintenance, and disposal of data.
5. It must be made clear to the individual that he or she is free to opt out of database listings both at the time his or her consent is sought and at any time thereafter.

According to NIH guidelines, the ideal process to obtain informed consent is as follows:

1. The data subject must be approached for consent at a time and location that is convenient and comfortable for the subject. It must be a private setting and one that allows the subject to ask questions freely.
2. The subject must be given adequate time to make an informed decision about whether to consent to the request for information. In the context of consent to experimental medical treatment, a minimum of 24 hours was suggested as an adequate time frame. It was recommended that the patient be given the opportunity to choose the time frame should external conditions prevent a decision within 24 hours.
3. The individual should also be encouraged to discuss the decision with other people who may be affected by the decision, such as family members. This is especially important in the context of marketing databases where disclosure of personal information may result in increased direct marketing mail and telephone calls.
4. Consent should be sought only from persons legally capable of giving consent.
5. Those in charge of the data-gathering project must ensure that the persons responsible for obtaining the consent of data subjects understand the importance of the "informed" element of the consent. This can be done by thoroughly questioning the data gatherers about the subjects' comprehension of what the database project will entail.
6. Once consent is obtained, the individual must be given a copy of the consent form and must be encouraged to keep the copy for future reference.
7. Where the individual is likely to be dependent on the data gatherer in some way (e.g., a store at which the customer shops regularly), extra care must be taken to explain that a refusal to consent to the data gathering will not prejudice the individual in future dealings with the data gatherer.

INSURANCE

"Although many of these disclosures are included on insurance application forms, these often appear in the form of small print and are phrased in a confusing manner."

By ensuring that the consent obtained from a data subject is truly an informed consent, the individual is given the sense that he or she is a partner in the venture and that his or her needs are not only being respected, but are the driving force behind the activities of the data gatherer. This, in turn, is likely to increase the cooperation obtainable from the subject as well as reducing the liability of the data gatherer.

The information presented on this topic is constantly evolving and should be monitored by the insurance industry. Consider, for example, a piece of legislation being considered in this area. The Medical Records Confidentiality Act, proposed in the 104th Congress, would, according to John Lobert, senior vice president of government relations for the National Association of Independent Insurers, require separate authorizations for as many as 20 different providers and parties involved in a property/casualty claim. [Gettlin, 1996] Companies like American Express have realized the potential for problems and have created a set of Consumer Privacy Principles for their employees. [Punch, 1994]

Ethical Issues in the Use of Information

After information is collected in a database, companies act on the data. They may use the data for many purposes: pure marketing research, commercial applications, and adversarial uses. Three legal principles are important to all categories of data usage. The first involves *ownership*. Both the common law and federal statutes begin with the premise that the data subject has no legal ownership rights over his or her personal data. This reality may conflict with what consumers desire, but still appears beyond dispute. Parties in possession of information about a consumer own the information so long as they came into possession of the information by legal means.

The second legal principle involves *discrimination* under civil rights laws. Information may not be used to discriminate unfairly against individuals or groups of individuals who fall into protected civil rights categories. A well-known example of a discriminatory practice is "redlining" in which minority groups are excluded from service areas. [Smith, 1995] Another less pernicious but still prohibited example is the exclusion of minority groups from offers of special promotional incentives. [Cepedes and Smith, 1993] In the insurance industry, state statutes also may govern what information can be used and how it can be used.

The third legal principle is that holders of data must provide *security* over personal information so that subjects (and data users) will not be hurt by unauthorized or unscrupulous uses of data. According to *Money* magazine, consumers have been defrauded out of hundreds of millions of dollars by companies misusing database information. [Simon, 1992]

Commercial Applications of Customer Data

Service to Existing Customers

The primary commercial justification for customer databases in a typical business is that information is needed to provide existing customers with better service. This use of data provides a clear benefit to the customer. At the same time, data-based service benefits the business as a tool in creating a more satisfying and more permanent patronage relationship.

In exchange for the value of their business, customers have a right to expect that their service providers will not harm them. They may have to reveal their deepest secrets about things like their financial status, medical conditions, and drug use. Often service providers choose to err in favor of *completeness* over *relevance* of the data, believing that more extensive "background" information enables them to deliver better service.

Professionals—such as physicians, attorneys, accountants, ministers, and psychiatrists—have set very high ethical standards for using customer data. Based on these professional role models, customers may feel they can expect similar standards of care from bankers, credit card companies, telephone companies, retailers, and insurance companies.

Developing a mutually beneficial relationship between client and service provider requires trust. Since establishing that trust, in turn, requires mutually ethical behavior, a business must understand the ethical expectations held by its customers. Consumers have every reason to assume that information in their files will remain *accurate* and *up-to-date* so that service will be appropriate. The consumer reveals personal information and has expectations that the data will be kept *confidential* and *secure*. If that trust is violated, consumers are unquestionably free to switch to other service providers, taking their patronage with them. In an age of "relationship marketing" where it costs five times as much to entice

INSURANCE

"Parties in possession of information about a consumer own the information so long as they came into possession of the information by legal means."

INSURANCE

"It makes little commercial sense to drive customers away by using their data in an insensitive way."

a new customer as to keep an existing customer, it makes little commercial sense to drive customers away by using their data in an insensitive way. [Montague, 1994]

Targeted Promotion

The second commercial use of customer databases is to target promotions to customers who are likely to be interested in purchasing a particular product. Some likely prospects may be found among a firm's present customers; other likely prospects must be found in additional databases. Targeting restricts the allocation of promotional effort to potential customers with high profit potential and, therefore, involves some "qualifying" or prioritizing.

In contrast to the uses in the next section, it is useful to note that the business, not the consumer, initiates the commercial contact. There is also no overriding societal interest in supporting a business's right to targeted promotion.

Any harm done depends on an individual's perceptions about how intrusive the promotion is. In contrast to mass promotions, one consumer may feel that personalized promotions, based on prior knowledge about the consumer, such as telephone calls or direct mail pieces that knowingly invade a person's home, are especially intrusive. Another consumer will see the information he or she receives about products and services in this way as one dimension of better service. In addition, the latter consumer appreciates the fact that he or she is not included in promotions for other products that are not of interest.

The Direct Marketing Association recommends a simple, blanket solution to the ethics of intrusion with regard to *notice* or *consent*. It recommends letting each consumer decide how much targeted promotion to receive and allowing him or her to "*opt out*" whenever he or she feels uncomfortable. As a practical matter, this approach would require the provider of information to give prior notice about any new uses of information and to request explicit consent from the consumer before using it.[2] After all, the people involved are customers or potential customers. There is no commercial benefit in upsetting them. If angered they might use their political clout to bring the wrath of the government down on an entire industry—whether that industry is the direct mail industry or the insurance industry.

The direct mail community currently is exhibiting preliminary evidence that marketers are treating consumer information as if the individual "owns" it and has the power to control its disposition. One proponent of that position is the futurist Joseph Clark. Individuals would be able to "opt out" of marketing programs, or choose to participate in exchange for some favor or privilege. [Edmondson, 1996; Laudon, 1996]

Adversarial Uses

Another category of uses for data is the opposite of targeting specific consumers for promotion inclusion—it separates those to be excluded. When used in this fashion databases and profiles can be used to identify people who are likely to be troublesome customers or even potential litigants against the company.

Screening Out

Completely avoiding potential customers is known as "screening out" or "qualifying." One example of this type of use is an insurance company that uses customer information to assess risk and then either excludes some consumers from coverage or charges them more expensive rates. Another example is that of credit providers who use information on an individual to deny credit. A third example is retailers who prevent people from acquiring products or services that they are not legally entitled to purchase, such as guns, pornography, alcohol, cigarettes, etc.

One characteristic of most industries that screens out is that demand for the product exceeds supply. In these markets, including insurance and credit, customers usually initiate the interaction with the business on the basis of a need that they recognize.

In the case of screening out, customers have a legal and ethical responsibility to reveal many types of personal and embarrassing information about themselves—the very information that may prevent them from getting what they want. To assure that the consumer has truthfully revealed the information, the business has been granted the right to use information from additional outside sources to verify the facts as revealed.

The Fair Credit Reporting Act of 1971 clearly enables companies to use databases to screen out. Consumers have little right to control the data files about themselves; certainly they do not have the right to restrict access from people who have a "legitimate business purpose."[3] Consumers have the right to have undisputed errors corrected and to explain their side to disputes, but they do not have an absolute legal right to what the con-

sumer perceives to be *accurate*.

For a fee, a consumer has the right to review the information in his or her credit record and to learn the identities of other parties who have accessed that information. However, there is no requirement that the keepers of the information must provide *notice* that other parties have accessed data. The utilitarian ethical view would argue that, since the selling agency has a right to the information in its possession, details of that information can be gathered ethically and shared without the consumer's *notice* or *consent*.

In itself, screening out can harm a consumer, especially if the consumer is not allowed to obtain something he or she needs. Such harm to individuals is justified ethically on the basis of broader social benefits. Industries such as the insurance industry and the lending industry provide essential services to society, and society recognizes their special role by protecting their "need to know" against an individual's right to privacy.

Tort Claims

When two parties sue each other, the law—and an ethical judge or juror hearing the cases—considers the facts with no prior judgment that one party's version of the case is more "honest" than the other's. The privacy of personal information is governed much more strongly by the civil courts than by any statutes. Attorneys are very adept at ferreting out information, and magazines run helpful articles showing how to protect one's assets from their grasp. For example see Novack [1995].

Eliminating Fraud

A final adversarial use of personal databases that is particularly important in insurance is the investigation and curtailment of fraud. The price tag for fraud was estimated to reach approximately $6 billion in 1995 for personal auto coverages alone. ["Tougher Stand . . .", 1997] Fraud prevention activities take casualty insurance into another dimension of ethics for three important reasons:

- First, since fraud has been determined by society to be criminal activity, the rules of the criminal justice system, which override individual privacy, become operative.
- Second, the balance of rights is different; when a fraud investigation arises during claims processing rather than underwriting, the two sides have equivalent rights. The insurer has the right to investigate; the claimant has the right to privacy.
- Third, fraudulent claims hurt all policyholders through higher insurance industry expenses and client premiums.

In summary, insurance companies have a socially mandated right to know about criminal behavior that is directed against their clients. Increasingly, society seems willing to take a stronger stand against fraud. In a survey conducted by Roper Starch Worldwide, Inc., 74 percent of respondents said they were willing to pay one extra dollar of premium on their auto policies to be used by law enforcement authorities in investigating and prosecuting fraud. The results in that survey also indicate that consumers are willing to provide additional information. The study found 88 percent of respondents would be willing to provide a copy of their car titles and 85 percent would be willing to bring their cars for inspection at the time the policy is taken out. ["Tougher Stand . . .," 1997] These results are consistent with a MasterCard International/Yankelovich Partners survey that demonstrated that many consumers would be willing to give up some privacy in exchange for better protection against fraud. [Loro, 1995]

If action is to occur based upon the evidence that public opinion supports a strengthening of anti-fraud enforcement activities, that action must be accompanied by a re-examination of the standards by which information is gathered and used. Fraud investigation by insurance companies for purposes of prosecuting perpetrators is essentially a quasi-public service. Ethical behavior in that role is more accurately judged against the standards developed for public officials involved with similar prosecutions. This will by necessity follow the same rules for the admissibility of evidence and, therefore, will be held to the same standards when collecting that evidence, as are public law enforcement officials. These ethical standards of society are much more fully developed in the law as a result of the court system's principal charge to interpret the Constitution.

Table 1 summarizes the discussion in this section. The headings across the top identify several uses of databases. The use that is least likely to harm an individual is "targeted promotion" from a typical business. The uses most likely to cause harm to an individual consumer are the "adversarial uses" shown in the two right-hand columns; in these cases companies hold a great deal of power—in the name of society.

INSURANCE

"The privacy of personal information is governed much more strongly by the civil courts than by any statutes."

Table 1
Practical Applications of Ethical Rules

Rules Governing Use	Customer Service	Targeted Promotion	Screening Out	Eliminating Fraud
Discrimination	Prohibited	Prohibited	Prohibited	Prohibited
Control Issues				
Ownership by Subject	None	None at Present	None	None
Access / Dissemination				
Subject Consent	Sometimes Required	Covered by "opt out"	Not Required	Not Required
Subject Notice	Sometimes Required	Covered by "opt out"	Upon Request; after-the-fact	Not Required
Data Security	To Protect Trust and Privacy	To Protect Subject Privacy	To Protect Data User's Interest	To Protect Data User's Interest
Content Issues				
Accuracy	To Assure Quality Service	To Assure Accurate Targeting	To Protect Business Interest	To Protect Business Interest
Completeness	Critical for Good Service	Helpful for Successful Targeting	To Protect Business Interest	To Protect Business Interest
Relevance	More Data May Support Better Service	To Assure Accurate Targeting	Cannot Be Determined a priori	Cannot Be Determined a priori
Currency	Critical for Good Service	To Assure Accurate Targeting	To Protect Business Interest	To Protect Business Interest

INSURANCE

"With adversarial information, the right and duty of an insurance company is to overcome individual privacy in pursuit of a broader social good."

The ethics associated with these last two columns do not stem from the potential for harm to a consumer. With adversarial information, the right and duty of an insurance company is to overcome individual privacy in pursuit of a broader social good. A potential conflict arises when data gathered for different purposes are combined: for example, when customer service records are combined with screening out data. The interest of the consumer and the interest of the company cannot both be maximized simultaneously. To nobody's surprise, the interests of the business dominate.

Unfair Discrimination

The headings on the left margin in Table 1 summarize the discussion of rules governing use of databases in this chapter: discrimination, control, and content. The table shows that discrimination is the clearest issue in that it is absolutely prohibited.

Control

The table also is clear about ownership: while consumers desire control over how their data are used, at present no legal authority supports the idea that consumers own information about themselves. Federal law has addressed consumers' concern in a very spotty way, as with the Video Privacy Protection Act. Many types of information are not covered: insurance records, genetic records, credit card retail transactions, rental and real estate records, financial records, criminal records, phone bills, welfare files, employment records, etc. [Laudon, 1996] At present the relevant laws are incomplete and differ from state to state. In many states, for example, consumers have no control over dissemination of their medical records and have no access to the records themselves.

The Direct Marketing Association provides a courteous and effective way to ensure consumer control through its "opt-out" policy. Many would like to see this policy applied to *notice* and *consent* regarding consumer service records, and an ethical argument to support this position would be easy to construct.

Potential ethical conflicts arise when data gathered for different purposes are combined. Insurance companies, for example, have access to client records, marketing databases, screen-

ing out data, and fraud information. Once facts are exposed by an adversarial database and copied into other databases, it is unlikely that the consumer can ever control information again in the way he or she would like. In a recent example, Lexis-Nexis discontinued after 10 days the practice of an online offering that provided access to social security numbers. [Flynn, 1996]

Content

Table 1 also shows a conflict between *relevance* ("only relevant data should be contained in the database") and *completeness*. To provide the best service—for example, medical care—the provider needs to know many things beyond the patient's stated symptoms. To root out fraud, any clue might be relevant.

Managing Information Ethically[4]

Because the insurance industry maintains virtually all its information in computerized form, this discussion would be incomplete without considering a set of issues surrounding today's information systems. In the information system domain, the broad ethical concepts that guide the planning, development, implementation, and usage of systems fall into three categories: responsibility, accountability, and liability. The generally accepted definition for these foundation concepts are as follows: *Responsibility* is based on the idea that "individuals, organizations, and societies are free moral agents who act willfully and with intentions, goals, and ideas." Therefore, they are morally responsible for their actions. *Accountability* is the ability to trace actions to identify individuals responsible for deciding to take those actions. *Liability* is the idea that people may be obligated by law to compensate those they have injured in some way; liability is established by law that provides legal remedies for proscribed behavior.

The ethical risks associated with information gathering, storing, and using are categorized into four areas and must be addressed when managing information.

Privacy:

The ability to determine when, how, and to what extent information is communicated to others.

Accuracy:

The extent to which information represents what it is supposed to represent.

Access:

The ability to obtain and make use of information.

Property:

The exclusive right to own and dispose.

While technology improves the gathering, processing, and manipulating of information, it is both a boon and a bane when it comes to managing ethical risks of information. For example, an individual's right to privacy is threatened in that personal data becomes potentially more accessible to a wider audience and is more easily transferable. As the individual is less involved in the recording of the information, the chances of recording inaccurate information also greatly increase. However, many have suggested that by automating information, fewer people are required to handle hard copies of the information, therefore reducing data errors and increasing data accuracy. [Benzing et al., 1994] Additionally, it is possible to use more sophisticated controls to protect electronic files from unauthorized access than are available for the protection of hard copies. All of these factors must be considered in a firm's plan to manage the risks associated with electronically stored data.

The full report addresses the following standard risk management steps as they relate to an insurer's information system:

- risk identification and analysis
- risk control
- risk financing

Conclusion

The research summarized in this article leads to several recommendations for the insurance industry as it deals with the ethical use of data in its own operations and by its insureds. For the most part these recommendations center on awareness regarding the value and sensitivity of data. Specifically the insurance industry is encouraged to recognize several factors:

- The privacy concerns of its customers are legitimate and the insurance industry must take appropriate steps to secure data.
- Careful data handling can be a competitive advantage. If you deserve it, take credit for doing it well.
- Almost every public policy activity of insurers, agents, and trade organizations can have secondary effects that deal with data and privacy.
- Rules governing the privacy of data will evolve from social values and will produce a body of common law.

INSURANCE

"The privacy concerns of its customers are legitimate and the insurance industry must take appropriate steps to secure data."

"Society inherently distrusts large organizations, including insurers. That distrust, in turn, implies that regulation of the insurance industry's data practices is a possibility.

- Society inherently distrusts large organizations, including insurers. That distrust, in turn, implies that regulation of the insurance industry's data practices is a possibility. One strategy to avoid unacceptable regulations in this area is to work proactively to develop a system that will provide the regulation.
- Decide where to go next!

Endnotes

1. The discussions at the Conference are presented in the book *Privacy and the Insurance Industry*, edited by Professors Harold D. Skipper Jr. and Steven N. Weisbart [1977].
2. An alternative would be the following test of conscience from Professor Mary J. Culnan, "Would you be comfortable sending a member of your family the same offers that you propose to send to your customers?" [Waldrop, 1994].
3. Most businesses believe they fall into this category, including landlords, retail stores, contractors, etc.
4. For a more detailed discussion of this topic see Brown, Gammill, Nielson, and Seville (1997).

References

Benzing, Lynn and Charles F. MacKelvie, "Coping with Patient Privacy: A Prescription for the Pharmaceutical Industry," *Pharmaceutical Executive*, Volume 14, No. 11 (November 1994), pp. 63-74.

Bloom, Paul R., George R. Milne, and Robert Adler, "Avoiding Misuse of Information Technologies: Legal and Societal Considerations," *Journal of Marketing*, Volume 58, (January 1994), pp. 98-110.

Brown, Daniel, Linda Gammill, Norma Nielson, and Mary Alice Seville, *Ethical Uses of Information in Insurance* (Malvern, Pennsylvania: Insurance Institute for Applied Ethics, 1997).

Carroll, John M., Confidential Information Services: Public and Private (Boston: Butterworth-Heinemann, 1991).

Cepedes, Frank V. and H. Jeff Smith, "Database Marketing: New Rules for Policy and Practice," *Sloan Management Review*, (Summer 1993), pp. 7-22.

Edmondson, Brad, "When Buyers Choose," *Marketing Tools*, (November /December 1996), pp. 24-25.

Flynn, Laurie, "Company Stops On-Line Access to Key Social Security Numbers," *New York Times* (June 13, 1996), p. 11.

Gettlin, Robert H., "Insurers Win Revisions in Medical Records Bill," *Best's Review-P/C Edition*. (July 1996), pp. 12, 107.

Hatch, Denison, "The Assisted Suicide of Database Marketing," *Target Marketing*, Volume 16, (1993), pp. 8-9.

Laudon, Kenneth C., "Markets and Privacy," *Communications of the ACM*, (September 1996), pp. 92-104.

Linowes, David F., "Changing Customer Concerns in the 1990s: The Privacy Issue," *Vital Speeches*, Volume 58, (January 1992), pp. 198-200.

Loro, Laura, "Downside for Public is Privacy Issue," Advertising Age, (October 2, 1995), p. 32.

Montague, Claudia, "Common Hazards, Commonsense Advice," *Marketing Tools*, (November/December 1994), pp. 48-49.

National Institutes of Health, *Beta-Blocker Heart Attack Trial: Guidelines for Obtaining Informed Consent*, (Bethesda, Md.: Department of Health, Education, and Welfare, Public Health Service, National Institutes of Health, 1978).

Novack, Janet, "Private Lives," *Forbes*, (June 19, 1995), pp. 138-142.

Nowak, Glen J.; and Joseph Phelps, "Direct Marketing and the Use of Individual-Level Consumer Information: Determining How and When 'Privacy' Matters," *Journal of Direct Marketing*, Volume 9, No. 3 (Summer 1995), pp. 46-60.

Punch, Linda, "When Big Brother Goes Too Far," *Credit Card Management*, (October 1994), pp. 22-28.

Prosser, William L., "Privacy," *California Law Review*, Volume 48, No. 3 (August 1960), pp. 383-423.

Simon, Ruth, "Stop Them from Selling Your Financial Secrets," *Money*, (March 1992), pp.98-106.

Skipper, Harold D. Jr. and Steven N. Weisbart, *Privacy and the Insurance Industry* (Atlanta, Georgia: Georgia State University, 1979).

Smith, N. Craig, "Marketing Strategies for the Ethics Era," *Sloan Management Review*, (Summer 1995), pp. 85-97.

"Tougher Stand on Insurance Fraud Endorsed by More Americans, Says Survey," (Wheaton, IL: Insurance Research Council), January 1997.

Waldrop, Mary J., "The Business of Privacy," *American Demographics*, (October 1994), pp. 46-54.