Paul N. Bloom, George R. Milne, & Robert Adler

Avoiding Misuse of New Information Technologies: Legal and Societal Considerations

A variety of new information technologies have emerged that clearly can improve the efficiency and effectiveness of marketing programs. However, the use of technologies such as computer matching or automatic order-entry systems to support marketing programs also can lead to legal and societal difficulties. The authors review the types of problems that marketers could encounter when using new information technologies. Particular attention is paid to the possibilities of being charged with (1) participating in collusive information exchanges, (2) maintaining an illegal "essential facility," (3) storing or transmitting inaccurate and harmful information, and (4) violating the privacy rights of individuals. They offer ideas about how marketing managers and researchers can reduce the chances of facing these types of problems.

Marketers have been expanding their use of new information technologies, which we define as hardware or software that can transmit, store, sort, or transform information at high speeds. A host of new information technologies (see the Appendix for descriptions) are now being steadily and productively used by marketing managers and researchers. For example, technologies such as computer matching, which compares data bases to identify individuals common to both, are being used to improve market knowledge and guide market targeting decisions. Other technologies, such as automatic order-entry systems, are being used to improve the speed and accuracy of responses to customer orders and inquiries. For example, these technologies can make it possible for retail clothing stores to change how they stock, display, and promote items during midseason on the basis of sales figures from early in a season (*Chain Store Age Executive* 1991).

Though the benefits of using new information technologies have been examined by several observers (Blattberg and Deighton 1991; Buzzell 1985; Glazer 1991; O'Callaghan, Kaufmann, and Konsynski 1992), little attention has been devoted to the legal and societal dilemmas that use of these technologies can create for marketers (Marx 1988). However, misuse of these technologies can have a major strategic impact on a company, damaging its reputation and limiting the amount of trust it can foster in relationships with customers, employees, channel members, and competitors. We attempt to provide guidance to marketing managers and researchers about how to recognize and avoid such dilemmas. The discussion is meant to have relevance primarily for *users* of new information technologies, with only secondary consideration given to issues relevant to creators or marketers of the technologies themselves. Covering topics such as trademark and copyright law, which are pertinent to the latter groups, is beyond the scope of this article (Menell 1987; Stern and Eovaldi 1984).

We begin by describing four case studies of situations in which marketers encountered difficulties because of the way they used new information technologies. These marketers were charged with price-fixing through information exchanges, monopolizing essential facilities, transmitting inaccurate and harmful information, and violating privacy rights. After presenting the cases, we provide an in-depth examination of each of the four types of charges that have been introduced, paying particular attention to the latest relevant legal precedents and statutes. Following this discussion, other potential problems are explored, such as encountering difficulties with existing or proposed consumer protection and environmental laws. We conclude by proposing guidelines for marketing practitioners and offering several ideas for further scholarly research contributions in areas delineated here.

Four Case Studies

Charges of Price-Fixing Through Information Exchanges: The Airline Tariff Recording System

Major airlines are among the most visible and effective users of new information technologies. Their computerized reservation systems are used to improve service delivery and help implement their pricing strategies. When an airline wants to alter a fare, it simply enters the fare electronically

Paul N. Bloom is a Professor of Marketing and Robert Adler is an Associate Professor of Legal Studies, Kenan-Flagler Business School, University of North Carolina at Chapel Hill. George R. Milne is an Assistant Professor of Marketing, University of Massachusetts at Amherst. The authors thank the *JM* reviewers for their helpful comments and Jonathan Bloom for his assistance with graphics. Financial support for this research was received from the Marketing Science Institute.

Journal of Marketing
Vol. 58 (January 1994), 98-110

in a data base operated by the Airline Tariff Publishing Company in Washington, DC, and the new fare then is entered instantly in the various reservation systems throughout the country. On some days, airlines can enter as many as 200,000 fare changes (Dahl 1991).

Entering fare changes by using sophisticated information technologies potentially provides many benefits to the airlines and their customers, including giving customers the ability to search more efficiently and effectively for travel choices. But many critics contend that a key benefit provided by the fare-entering system is an improved capacity to collude and fix prices. In response to these criticisms, the U.S. Department of Justice recently filed price-fixing charges against the major airlines (Sanchez 1992). Moreover, a major class-action lawsuit—in which a U.S. Federal District Court certified domestic ticket purchasers as the largest class ever certified in a class action in this country—was filed previously against nine airlines and the Airline Tariff Publishing Company (*In re Domestic Air Transportation Antitrust Litigation* 1990).

The Justice Department and plaintiffs in the class action suit asserted that an airline will enter planned fare cuts into the system, but retract them before the fares are actually available if a competitor retaliates by immediately entering lower fares in the system, perhaps on other, highly profitable routes of the first airline. Through these back-and-forth computer "signals," the airlines can "police" each other's fare cuts, leading to higher fares than would be the case without the computerized reservation systems.

The final outcome of these lawsuits should be determined soon. Several of the airlines have agreed to out-of-court settlements that await final approval. The airlines pledged to discontinue submitting fare cuts before the fares were actually available for purchase. They also agreed to stop several other practices, such as using two-letter codes when entering fare changes, which would identify toward whom a change or retaliation was "aimed" (Nomani 1991a, b). Finally, the airlines agreed to provide all class members who make claims with up to $408 million in certificates entitling them to discounts on future flights (of approximately 10% off). The number of certificates received will depend on how much a claimant flew between January 1, 1988 and June 30, 1992 (Pulley and O'Brian 1992).

Charges of Monopolizing Essential Facilities: Microsoft

Microsoft is both a creator and user of new information technologies. As one of the most successful companies of the last decade, it has received considerable scrutiny from researchers, competitors, the press, and others. Recently, the Federal Trade Commission (FTC) has been conducting a major investigation of Microsoft, examining whether any anticompetitive acts have been used by the company in achieving its enormous success. Among the areas the FTC is reported to be investigating is how Microsoft uses its dominance in the provision of operating systems for PCs (i.e., MS-DOS and Windows) to dominate the market for applications programs for PCs as well. It has been alleged that Microsoft favors its own applications program developers by providing them with information about pending changes in the operating systems long before it reveals this information to competing developers (e.g., Borland, NeXT) (Davidson and Zachary 1993; Rebello 1993).

One way of interpreting this charge against Microsoft is as a complaint about how the company is using its monopolistic control of the "essential facility" of the operating systems to gain control of another market (i.e., the applications program market). Concern about companies leveraging control of one market into control of another has led to the emergence of an "essential facilities doctrine" under antitrust law. This doctrine was used, for example, to allow MCI access to AT&T's local telephone lines (*MCI Communications v. AT&T* 1983). This doctrine provides the opportunity for competitors who feel improperly restricted in their access to customers because a major competitor controls a "facility"—a term that has had many interpretations (see next section)—to complain to the antitrust enforcement agencies or file suit themselves to obtain use of the facility.

At this time, it is unclear how far the FTC plans to go in pursuing this case (Davidson and Zachary 1993). There are some people, such as Steve Jobs of NeXT, who would like to see the alleged favoritism stopped by breaking Microsoft into two companies, one that would sell systems software and another that would sell applications software (Cauley 1993). Clearly, Microsoft has suffered already from this episode by incurring considerable legal expenses and negative publicity. We see the potential for other companies—even those solely involved with the use of new information technologies—to face the same kind of antitrust troubles if they are too successful in controlling certain markets. For example, the major airlines were forced to give smaller airlines better access and more favorable treatment in their computerized reservations systems because of an "essential facilities" challenge (see next section).

Charges of Transmitting Inaccurate Information: TRW

New information technologies have permitted a large number of information services companies to prosper, many of which supply data that other organizations use to guide them in designing and promoting their products. These companies have developed huge data bases that contain information ranging from credit histories to records of consumer purchases and medical histories. Many organizations seek access to these data bases to gain names for mailing lists or to screen customers.

TRW, a large credit-reporting business, recently found itself the target of charges that it stored and transmitted inaccurate information. In 1991, six state attorneys general and the FTC filed suits claiming that TRW failed to follow reasonable procedures, required by the Fair Credit Reporting Act (1970) and other state statutes, to ensure a sufficient level of accuracy in its consumer credit files. The government also accused the company of inadequately investigating consumer complaints about inaccuracies and allowing errors to recur in consumer files (Miller 1991a; *Texas v. TRW, Inc.* 1991). According to the suit, TRW's poor record keeping resulted in lost credit and employment opportuni-

ties for consumers, especially those with good credit records whom the company confused with consumers with similar names but bad credit records.

Though TRW originally contested the suits and even filed countersuits against two attorneys general challenging their authority to sue the company (*TRW, Inc. v. Texas* 1991), the company quickly agreed to a consent order to end the controversy and reduce the negative publicity it was receiving. It pledged to implement new systems to monitor accuracy and resolve complaints within 30 days after receiving them, and to pay legal costs in the state cases.

Charges of Violating Privacy Rights: Blockbuster Video

The lucrative opportunities in the information services business have attracted the interest of many companies that have their primary businesses in other areas. Supermarkets, financial institutions, magazines, mail order houses, and even doctors (Miller 1992) have learned that the data they routinely accumulate about their customers has considerable value to other organizations. One company that initially saw an attractive opportunity in selling its data was Blockbuster Video. As it investigated further, however, it faced a torrent of criticism.

Though the federal Video Privacy Protection Act (1988) prohibits video rental dealers from revealing to anyone the titles that an individual rents, Blockbuster reportedly believed that it still could sell data about the *categories* of movies that its customers rented (e.g., drama, comedy, foreign) without violating the law. One of its executives, in a *Wall Street Journal* interview, stated that the company contemplated compiling and selling such information (Miller 1990). This report provoked a storm of protest from people concerned about infringements on the privacy of Blockbuster customers such that the company quickly retracted the idea and claimed the executive spoke without authority (Hume 1991; Radding 1991). Interestingly, the protest reached a feverish pitch despite the fact that Blockbuster Video does not rent X-rated movies.

Blockbuster received considerable negative publicity for considering an action that was within its legal rights. It found itself buffeted by the growing concern about infringements on privacy rights, and it paid a serious image price for this contemplated action.

Current Legal Developments

Depending on the specifics of their behaviors and the conditions in the markets in which they compete, other new information technology users could face problems similar to those encountered by the airlines, Microsoft, TRW, and Blockbuster Video. Aside from subjecting themselves in the short run to costly disruptions and legal fees, companies can suffer long-term damage to their reputations and relationships with key markets and publics. To avoid these problems, it should be helpful to review the following sections, which cover the legal developments in the four areas introduced in the case studies. Table 1 summarizes the relevant legal statutes under each of these areas.

TABLE 1
Relevant Statutes for Users of New Information Technologies

Potential Problem Area	Statutes
Collusive Information Exchanges	Sherman Act, Section 1 FTC Act, Section 5 State Antitrust Statutes
Essential Facilities	Sherman Act, Sections 1 and 2 FTC Act, Section 5 Civil Aeronautics Board Rules (1984) State Antitrust Statutes
Inaccurate Information	FTC Act, Section 5 Fair Credit Reporting Act (1970) State Antitrust Statutes State Product Liability Laws State Defamation Laws
Privacy Threats	Video Privacy Protection Act (1988) Fair Credit Reporting Act (1970) Privacy Act (1974) Right to Financial Privacy Act (1978) Computer Matching and Privacy Act (1988) Cable Communications Policy Act (1984) Telephone Consumer Protection Act (1991) State Caller ID Rules State Privacy Laws
Other Potential Problems:	
Use of Offensive Technologies	Telephone Consumer Protection Act (1991) State Laws
Deception	FTC Act State Laws
Environmental Protection	State and Local Laws

Legal Treatment of Information Exchanges

As alleged in the airline price-fixing cases, new information technologies can make it easier for competitors to monitor and police one another, facilitating collusive behavior. When one competitor knows that other competitors can learn almost instantly about its marketing actions, the incentive for taking such actions could be diminished (Salop 1986). The competitor may not want to be aggressive if doing so would trigger immediate, financially harmful retaliatory actions. A general disincentive to engage in price-cutting strategies easily could result in a tacit or even an overt agreement to fix prices, allocate customers, restrict promotional initiatives, or avoid other forms of aggressive marketing.

The antitrust enforcement agencies have a long history of scrutinizing information exchanges among trade association members and by other organizations such as the Airline Tariff Publishing Company. Several classic cases have found these activities to be part of a pattern of illegal collusion (Stern and Eovaldi 1984). For example, an "open com-

petition'' plan adopted by a hardwood producers association, which sought to keep all members informed of prices being charged, constituted illegal anticompetitive behavior in the eyes of the courts even though the companies made no explicit agreement to fix prices or restrict output (*American Column and Lumber Company v. U.S.* 1921). Similarly, in *U.S. v. Container Corporation of America* (1969), a tacit agreement to exchange data about current prices or prices last quoted to particular customers among producers of corrugated containers was declared illegal. Direct exchange of current price information, accomplished through telephone calls from one company to another, also was found to be collusive in a case involving four leading gypsum companies (*U.S. v. United States Gypsum Co.* 1978).

These cases suggest that though the courts generally have required that a collusive agreement exist before they will find violations of Section 1 of the Sherman Act, certain types of information sharing will be viewed with a skeptical eye (Stern and Eovaldi 1984). According to one antitrust observer (Givens 1989, p. 142–2),

> Exchanges of many types of information, especially concerning historical, rather than current, economic activity have been upheld as permissible where a third party collects the data and participants are not individually identifiable. However, the exchange of very recent or current prices or customer information may be dangerous and violate the Sherman Act if it can be found to have potentially anticompetitive effects.

In particular, if companies share data among themselves but withhold it from their customers, the courts have viewed the information exchange more suspiciously (Stern and Eovaldi 1984; Wilcox 1971).

Therefore, a firm that participates in certain types of information exchange systems could invite antitrust action. Antitrust liability could be particularly high if anything else about a firm's interactions with its competitors can be construed as evidence that a formal collusive agreement exists. A recent example that illustrates how strong antitrust challenges still can be mounted against information exchange systems involved the eight Ivy League universities plus the Massachusetts Institute of Technology (MIT). The regular exchange of information about the formulas each school used to make financial aid awards drew the attention of the Justice Department. This practice was challenged in an antitrust suit because it appeared to be part of a collusive pattern that allegedly also included collusion on tuition rates and faculty salaries. In a recent settlement of this case, the Ivy League schools agreed to discontinue many of their joint practices (*U.S. v. Brown University et al.* 1991). MIT, however, contested the charges and was found in a federal lower court ruling to have illegally fixed prices (Ingrassia 1992). This decision is being appealed by MIT.

Legal Treatment of Essential Facilities

We foresee challenges similar to the one facing Microsoft, coming from either government or smaller competitors, arising when there are reservation systems, automatic order-entry systems, payment systems, or other technologies that become the dominant mechanism through which sellers carry out transactions with customers (Marx 1988). As we discuss subsequently, however, the circumstances under which these ''essential facilities'' challenges will be successful are limited.

The essential facilities doctrine was first established in *U.S. v. Terminal Railroad* (1912). In this case, the Supreme Court ruled that a group of railroads that had gained control of a switching station at a crucial location in St. Louis had to allow other railroads use of the facility. Since this case, the doctrine has been applied to permit competitors to gain access to the Associated Press wire service (*Associated Press v. U.S.* 1945), a multi-day ski lift ticket in Aspen, Colorado (*Aspen Skiing v. Aspen Highlands* 1985), electric transmission lines (*Otter Tail Power v. U.S.* 1973), natural gas pipelines (*Consolidated Gas v. City Gas* 1987), and computerized reservation systems owned by the major airlines (*United Airlines et al. v. Civil Aeronautics Board* 1985). In this last case, the major airlines were ordered not to do the following:

1. Favor their flights by displaying them before revealing other airlines' flights,
2. Charge different booking fees to different airlines, or
3. Limit connecting flight information of competitors in ways designed to confuse or mislead consumers (Guerin-Calvert 1989; *Harvard Law Review* 1990).

In *MCI Communications v. AT&T* (1983), the Seventh Circuit Court of Appeals set forth what generally is considered the most modern explication of the requirements for establishing an essential facilities violation of the Sherman Act (under Sections 1 or 2). In allowing MCI access to AT&T's local telephone lines, the court outlined four critical elements:

1. Control of the essential facility by a monopolist;
2. A competitor's inability practically or reasonably to duplicate the essential facility;
3. The denial of the use of the facility to a competitor; and
4. the feasibility of providing the facility.

In addition, the doctrine can be applied only when allowing access to the facility would result in improved competition (Areeda and Hovenkamp 1989).

The essential facilities doctrine continues to evolve (Hylton 1991; Podell 1989). For this reason, it is difficult to predict how the courts might treat a case involving (1) firms that are not utilities—which clearly are monopolies—or (2) firms that are not involved in an overt conspiracy. Though several lower courts have found the maintenance of essential facilities by nonutilities to be illegal attempts to monopolize under Section 2 of the Sherman Act, the Supreme Court has yet to rule on the issue (Podell 1989). For example, the defendant in the *Aspen* case was found by a lower court to violate Section 2 through monopolizing an ''essential'' ski lift pass, but the case was decided on different grounds at the Supreme Court level. Moreover, the other case argued before the Supreme Court that involved a nonu-

tility and the essential facilities doctrine, the *Associated Press* case, produced a ruling that an illegal combination of firms existed, behavior covered by Section 1 rather than Section 2 of the Sherman Act.

Nevertheless, a Section 2 charge against a nonutility might be upheld under the right circumstances. Moreover, it is possible that unduly restrictive access to an essential facility could be viewed as an unfair method of competition under Section 5 of the FTC Act, as can be argued in the Microsoft case.

Though the Microsoft case involves the marketer of a new information technology itself, not just a user of these technologies, we can foresee similar cases being brought against the latter type of firm. A smaller competitor might seek access to a highly successful automatic order-entry system or a reservation system that would be extremely difficult and expensive for it to duplicate on its own. As is the situation with price-fixing charges, how the courts would treat such a case might depend on whether a series or pattern of anticompetitive behaviors occurred.

Legal Treatment of Inaccurate Information

As demonstrated in the case against TRW, companies using new information technologies to store and transmit credit records must meet the requirements of the Fair Credit Reporting Act. Supplying inaccurate credit information can lead to sanctions and fines under this Act. Under its provisions, consumers have the right to obtain for a reasonable fee from any credit reporting agency their own credit reports and the names of parties who have received the reports. They also can request investigations of inaccuracies and add statements to their reports indicating that they dispute the accuracy of specific information.

Currently, there are numerous parties calling for strengthening of the Fair Credit Reporting Act, including several major credit reporting companies (Miller 1991a). In addition to seeking more privacy protection (discussed subsequently), advocates of reform have called for revisions such as requiring credit reporting agencies to provide free annual copies of consumers' credit reports on request, imposing stiff fines on banks and retailers that submit erroneous data about consumers, and setting tighter rules and time deadlines on credit reporting agencies for investigations of inaccurate information (Miller 1991a).

Interestingly, the Fair Credit Reporting Act extends only to credit transactions. The storage and transmission of inaccurate non–credit-related information is not regulated by any specific statutes. But inaccurate information can lead to individuals being unfairly denied jobs, promotions, or insurance, or they can be placed on mailing or telemarketing lists they find distasteful or intrusive.

Similarly, companies can be harmed seriously when they rely on inaccurate information in data bases. They can waste money contacting the wrong people, or they can make costly strategic mistakes by relying on false data. For instance, a firm might fail in introducing a new product to a region because it relied on inaccurate reports about the financial well-being of several key customers in that region.

Until more sweeping legislation is passed, legal challenges to the storage and transmission of inaccurate information could come from several directions. One possibility is that the FTC or individual attorneys general could generally challenge an action as an unfair or deceptive practice under the FTC Act or under a state "baby FTC Act." For example, several attorneys general used their baby FTC Acts to file charges against TRW in the cases discussed previously—though before settling TRW contested the legality of using these statutes (*TRW, Inc. v. Texas* 1991).

Another possibility is that product liability laws could be used to deal with inaccurate information. Use of the product liability laws for this purpose has grown substantially in recent years (Marx 1988). For example, in *Brockelesby v. United States* (1985), the families of six crew members (who were killed when, relying on a flight chart containing faulty information, their plane crashed into a mountain in Alaska) recovered nearly $13 million from the U.S. Government and a map company. That inaccurate information leading to death or injury could raise liability concerns was not new to the map company. It had previously lost a lawsuit also involving a fatal crash caused by a defective map (*Aetna Casualty and Surety v. Jeppesen* 1981).

In a related occurrence, inaccurate weather information issued by the government resulted in liability when eight fishermen relied on the information and died when they confronted 100 mile-per-hour gusts and 60-foot waves (*Brown v. United States* 1984). The government had neglected to repair an electronic data buoy that likely would have alerted the weather service to the storm's approach (Marx 1988).

Still another legal challenge to the use of inaccurate information could come in the form of defamation suits (Marx 1988). Indeed, new information technologies have the potential of increasing the incidence of such suits. They do so because they can spread defamatory information more widely and quickly than old technologies. Furthermore, their sophistication and complexity offer more opportunities for mistakes. Thus, defamation suits such as *Dun and Bradstreet v. Greenmoss Builders* (1985) could emerge. In this case, the U.S. Supreme Court upheld the imposition of punitive damages against Dun and Bradstreet for libeling Greenmoss Builders through an erroneous credit report.

Given the possible legal liabilities that exist, a company may want to do what it can on its own to eliminate inaccurate information. For instance, it could invite regularly individuals and institutions either to review and correct their data files or remove themselves completely from the files. Several major financial services companies (e.g., American Express) offer such invitations to their customers.

Legal Treatment of Privacy Threats

Blockbuster Video operates in one of the few industries in which privacy protection legislation exists in the United States. The Video Privacy Protection Act of 1988, which prevents retailers from revealing the titles of films that people have rented, is one of the very few federal laws designed to

protect individual privacy.[1] The Fair Credit Reporting Act (1970) also offers privacy protections for individual consumers, but it has been criticized for having numerous shortcomings.

Beyond these statutes, most of the federal laws in the privacy area are designed to prevent privacy intrusions by governments, not by businesses or individuals (e.g., Privacy Act of 1974; Right to Financial Privacy Act of 1978; Computer Matching and Privacy Act of 1988). Moreover, the privacy protections in the Constitution (e.g., the Fourth Amendment's prohibition on "unreasonable searches and seizures" and the Fifth Amendment's right against self-incrimination) generally cover only governmental abuses. Private companies do not violate constitutional proscriptions when they engage in behavior that would be clearly improper for government agencies. Accordingly, most private sector activity remains unregulated (Simitis 1987; Peck 1984).

The paucity of federal privacy laws has contributed to a growing clamor for more privacy regulation. Thus far, this clamor has produced numerous legislative proposals but only a few laws and regulations, mainly at the state level. Public support for action, however, appears to be strong. A 1990 Harris poll found that 79% of American voiced concerns about threats to personal privacy—an increase of 15% over a similar poll in 1978—and 49% stated that they were "very concerned" (Equifax 1990). Similarly, a 1991 Gallup/*Advertising Age* poll found that 45% of the respondents described themselves as "very concerned" about what marketers can know about them, and 33% said they were "somewhat concerned" (Hume 1991). Treatment of the privacy issue in the popular press and best-sellers such as *Privacy for Sale* (Rothfeder 1992) seems bound to keep public concern high. Hence, more substantial federal legislation could be on the horizon.

The case of Caller ID. One recent new information technology, Caller ID, has stimulated privacy debates throughout the United States (Smith 1989). These debates have examined issues that also seem likely to arise in considering a variety of other forms of privacy legislation. Thus, a review of how Caller ID has been treated can provide a clue to how more sweeping privacy-protection laws might be formulated.

Caller ID (see Appendix) offers benefits to businesses beyond providing the identities of their callers. When combined with computer matching capabilities, Caller ID allows companies to determine the name, address, credit rating, credit card number, and the like of the caller before answering. This technology has the potential of lowering response times and costs for direct marketing and customer service operations. It also affords the opportunity for marketers to add information to their data bases about the shopping behavior of individuals, because even inquiries (not just purchases) can be noted in a person's records. More complete pictures of individual shopping behaviors could be desired, not only by the companies that originally record the information, but also by marketing researchers and direct marketers from other companies, who may be willing to purchase this information.

The introduction of Caller ID has raised two fundamental issues:

1. Should a company be allowed to acquire and store information about individuals without their knowledge or consent?
2. Should a company be allowed to disclose information about individuals to other parties without their knowledge or consent?

Indeed, these same questions arise in considering the effects on privacy of using technologies such as computer matching or automatic order-entry systems. With respect to Caller ID, critics argue that this technology presents a major threat to individual privacy, and they seek to prevent users of it from acquiring consumers' telephone numbers (and therefore names and other data) without permission. They also seek to prevent disclosing information to others without permission (Caller ID Technology Hearing 1990). Many have called for a "blocking" feature, which would allow the caller to disable the Caller ID mechanism before making a call. The blocking feature could disable all calls coming from a particular phone line or disable calls on a per-call basis. Several states, including California, have allowed Caller ID to be introduced only if blocking is allowed (California H.B. 1446, Ch. 483). A recent listing of the state laws pertaining to Caller ID is available in the *Telemarketer's Guide to State Laws* (Direct Marketing Association 1990b).

Supporters of Caller ID have resisted blocking and permission requirements. They argue that these add to the cost of using the technology, countering the efficiencies the technology was designed to offer. They recognize that a few people might be harmed by allowing unrestricted use of Caller ID, as their shopping and telephone habits are revealed to employers, creditors, or direct marketers without their knowledge or consent. But they reason that any harm will be balanced by the benefits of having faster response times, lower costs, better marketing research data, and more tailored and efficient promotional programs. They also believe that harm can be mitigated by having direct marketers offer to remove from lists those who do not wish their names to be on them, something that is done routinely already by many direct marketers.

Thus far, it appears that the critics of Caller ID are winning. The technology has failed to gain approval in several states, and in those places where it has been allowed, there are requirements to have either blocking or permissions. It also has been declared in violation of Pennsylvania's Constitution by the Pennsylvania Supreme Court, where it was found to be illegal under the state's wiretap law (Geyelin and Carnevale 1992).

These outcomes may portend what is likely to happen when more broadly applicable privacy protection legislation is passed. Under such legislation, companies that store information about people could be forced to provide a "blocking" feature that allows individuals to avoid having information about them recorded. And once they give permission to have information about them recorded in a data

[1]This law came about when newspaper accounts listed the films rented by Supreme Court nominee Robert Bork. Almost immediately after the story broke, legislation was passed prohibiting the public disclosure of video rental information (Consumers Union 1991).

base, they also may have to be asked for permission to have their names and related information passed on to another party.

Other privacy legal developments. Several industry-specific federal laws have provisions analogous to the blocking and permission requirements of some state Caller ID laws. In addition to the previously mentioned Video Privacy Protection Act (1988), there is the Cable Communications Policy Act of 1984. Among other things, this act requires cable companies to notify their subscribers and obtain their consent whenever they collect information that will identify personally the subscribers. In addition, the Fair Credit Reporting Act (1970) allows credit reporting agencies to disclose information about consumers only for a legitimate business reason. This restriction could be narrowed if proposed legislation is passed. For example, several bills have been introduced in Congress that would make it difficult or impossible for credit information to be disclosed to develop lists, used by credit card marketers and others, which provide the names of people who have been prescreened for credit-worthiness (*Antitrust & Trade Regulation Report* 1991).

At the state level, various privacy protection laws have been enacted:

1. California has a law that prevents the commercial use of personal information created from state-agency transactions (e.g., automobile registrations, property transfers) (Direct Marketing Association 1990a).[2]
2. Maryland prohibits retailers from requiring (1) phone numbers from people when they sign credit card slips and (2) credit card numbers from people when they pay by personal check. These laws were designed to make it more difficult for retailers to do computer matching or other data searches to identify targets for direct marketing efforts (Maryland Commercial Law § 13-318; § 13-317).

Additional federal and state laws with similar features can be expected, all of which should make it increasingly difficult to formulate data bases and mailing lists. Eventually, the United States could follow in the direction the European Community seems to be headed, which would involve broad and sweeping privacy protection rules. A 1990 "Draft Umbrella Directive on Data Protection" offered by the European Community has the following requirements:

1. Data use is prohibited without permission of consumers;
2. Data subjects must personally be notified to whom personal information has been passed and for what use;
3. Data subjects can claim compensation if data is "misused and caused damage"; and
4. European Community data can be transferred out of the European Community only if the receiving country can guarantee the same level of protection as the EEC (di Talamo 1991).

Restrictions such as these would be troublesome to many in the United States, particularly direct marketers and marketing researchers (di Talamo 1991).

[2]This law was enacted in response to the death of actress Rebecca Schaeffer, who was located by her killer through California Department of Motor Vehicles information.

Our expectation is that, in spite of objections from certain parties, some form of general privacy protection legislation will be approved in the United States in the next few years, though in a less strict form than that proposed in Europe. One alternative approach to "soften" the European Community's prior authorization or notification requirements would be using "negative option" rules, in which people are assumed to consent to the use of personal information about them unless they mark a box or transmit a message indicating that they object. The use of negative-option rules appears to be how the Canadian government plans to improve privacy protection (Stacey 1992).

One major reason we expect approval of general privacy-protection legislation is because we believe the business community, with a few exceptions, will support such legislation. General federal legislation could preempt the confusing and conflicting assortment of state laws that are emerging. It also could eliminate the need to have industry- or technology-specific laws, many of which tend to be hard for government agencies to enforce and businesses to implement. Furthermore, under new privacy protection laws, direct marketers actually might become more efficient, because they would be contacting only people who clearly wanted to be contacted (Herring 1992). Moreover, new legislation could help legitimize marketing researchers, who could obtain better response rates to surveys as people become less wary about responding to telephone and mail requests.

A final reason the business community might support "negative-option" or other moderate privacy protection legislation is its desire to avoid even stronger legislation. Several states and the U.S. Congress, for example, have debated "do not call" laws, which would allow individuals to put asterisks next to their names in telephone directories indicating their desire not to be solicited or queried via the telephone. Marketers could be prosecuted and fined for not respecting those marks (Honomichl 1992; Birnbaum 1991). Rules recently adopted by the Federal Communications Commission under the Telephone Consumer Protection Act of 1991 do not go quite this far, merely requiring telemarketing companies to maintain their own lists of people who do not want to receive calls and prohibiting them from making calls to homes before 8 A.M. and after 9 P.M. Violators of these rules can be fined up to $500 per incident (Carnevale 1992; *Consumer Report News Digest* 1992).

Even without new laws and regulations, marketers may have to face legal action or fines if they call people who desire not to be called. A recently formed group, Private Citizen, provides a list of its members to businesses, putting the businesses on notice that its members do not want to receive calls and that any call to a member will constitute an acceptance on the part of the caller of a business agreement to pay the member a fee of $100 (Bowers 1991). Robert Bulmash, president of the group, recently won a court decision against a company that refused to remove his name from its lists and continued to call him (Miller 1989).

While awaiting the outcome of the various legislative and legal initiatives in the privacy area, it may be wise for marketers using new information technologies to treat pri-

vacy as an ethical issue as well as a legal one. Historically, it seems that those firms that have considered the ethics of storing and selling personal information have relied on the utilitarian argument of the greatest good for the greatest number to justify their behavior. They have argued that the direct marketing industry has prospered by storing and selling personal data and that this has created numerous jobs as well as lower prices and better service for the many customers who enjoy patronizing this industry. They have seen these benefits as outweighing the occasional harms that have come to people because they have received unwanted solicitations or have had information about themselves revealed to those who seek to hurt them (Culnan 1992).

However, more firms seem to be recognizing that they may have been overstating the benefits of their data management practices and understating the harms those practices can create. Several companies (e.g., Equifax, Fidelity) recently have announced that they will restrict dramatically the selling of information about individuals and others (e.g., Blockbuster, Lotus) have curtailed information-selling plans before they were implemented (Culnan 1992; Miller 1991b; Wilke 1991). These firms are realizing that it could be more advantageous to solicit only people who say they want to be solicited (Herring 1992). At the same time, they also are realizing that even strict controls on who can access private information can be avoided or ignored by those with criminal intent, leading to outcomes such as blackmail and worse (Rothfeder 1992). Thus, many firms may find that they feel more comfortable with the policy of being extremely restrictive about sharing private information. They may want to include sections on privacy in company codes of ethics or subscribe to industry codes (e.g., the Direct Marketing Association's "Mail Protection Service") to help them avoid problems in the privacy area.

Other Potential Legal Problems

Depending on the new information technology used by a marketer, several other legal and societal problems could emerge. The technology itself could be viewed as offensive or annoying to people and its use could be regulated or banned. Automatic dialers with computerized messages, which are used by telemarketers, provide an example of a technology that many find offensive. New rules promulgated by the Federal Communications Commission under the Telephone Consumer Protection Act of 1991 prohibit the use of artificial or recorded voice messages unless (1) the call is for an emergency, (2) the called party has consented previously to receiving such calls, or (3) the caller is a market research organization or a pollster.[3] The rules also prohibit unsolicited advertising by fax (Carnevale 1992; *Consumer Report News Digest* 1992). More restrictive regulations than these have received serious consideration at both the state and federal levels (Farhi 1989).

[3]Enforcement of the rules is being held up by a court injunction stemming from a lawsuit filed by a chimney sweep company in Oregon. The company says the rules discriminate against small businesses who find automatic dialers to be very efficient (Carnevale 1993).

New information technologies also can have the potential to contribute to efforts to mislead or deceive consumers. We can envision companies using capabilities like virtual reality to create an inaccurate picture of a product's features. Or the technologies could make it difficult for consumers to acquire the information they need to make an informed choice. The technologies also could dazzle and excite consumers in a manner similar to what fast-talking salespersons can do, and this could lead consumers to make purchases they later regret. Technologies that produce these kinds of outcomes could create liability for marketers under consumer protection statutes such as the FTC Act. FTC trade regulation rules also could come into play, such as those governing mail-order sales or "cooling-off" periods (when people can get their money back) after purchases from door-to-door salespeople.

A final area in which legal problems could emerge for users of new information technologies relates to environmental protection. For example, the use of computer matching to generate mailing lists could be seen as facilitating the distribution of tons of unwanted and unnecessary "junk mail." Because much of the paper in this type of mail is difficult to recycle, information technologies could be viewed as indirectly contributing to the solid waste disposal problems facing many communities. To date, environmental groups have been reluctant to lobby for more restrictions on junk mail, because they are such heavy users of it themselves when they do fund-raising (*Marketing News* 1990; Miller 1991c). This point is illustrated by the revision of the command from "stop junk mail" to "stop unwanted junk mail" in the environmentalist bible, *50 Simple Things You Can Do to Save the Earth* (*Marketing News* 1990). However, it seems plausible that some activist groups will support restrictions on the creation of lists in the hope of reducing the tide of junk mail.

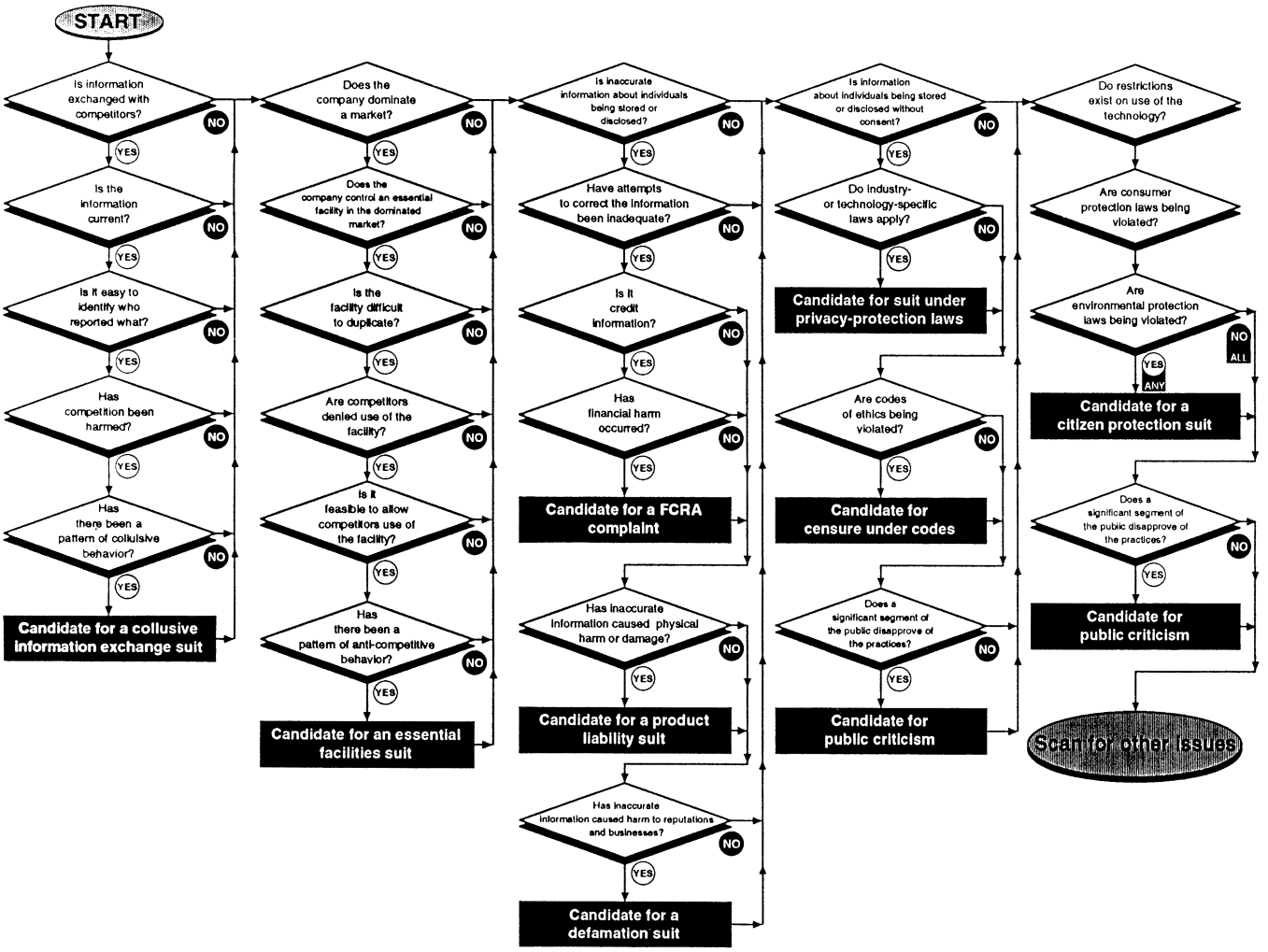
Managerial Guidance

Figure 1 contains a flow diagram that marketing practitioners could use to guide them to judgments about the extent of the legal and societal problems they are likely to encounter in using a particular new information technology. The diagram presents a checklist of questions, corresponding to material discussed here, that can help managers assess the likelihood of becoming a candidate for different types of legal and societal challenges. Each of the five columns of the diagram covers one of the problem areas covered in the previous sections. The questions should be addressed sequentially. Affirmative answers suggest a need to probe further in a problem area, whereas negative answers suggest that the next problem area can be examined.

An illustration of how the diagram can be used is a hypothetical situation involving a manufacturer of athletic sportswear. Assume this company uses new information technologies in the following ways:

1. It places tags with bar codes on all items so that they can be scanned by retailers, giving the manufacturer instantaneous information on the movement of items.
2. It places terminals in the warehouses of major retailers, which contain software that automatically enters orders

FIGURE 1
Question Sequence for Identifying Legal and Societal Problems



with the manufacturer on items that are running low (as determined by the scanner data). Retailers also can trace the performance of items very easily on these terminals.

3. It captures the credit card numbers used in retail credit purchases and then matches these numbers with names and addresses using the services of a mailing list house. Lists of people who have bought their brand of sportswear are then sold to several sports-oriented mail-order catalogues.

Using the diagram, the company first would consider whether information obtained from scanners about retail sales (and prices) was being shared with competitors. If no one other than the retailers and the manufacturer had access to these data, then the remainder of the questions in the far left column could be ignored and the essential facilities questions in the second column could be addressed. Here, the company first would consider whether it could dominate the athletic sportswear market or some portion of it. If it determined that it was a dominant firm in, for example, the running shorts market, then it would have to consider whether the automatic order-entry system created a situation in which the major retailers tended to want to order running shorts only through this system. Assuming this was not the case, the third column questions on inaccurate information then would be considered.

If the first question about inaccurate information would be answered negatively, then the next column's privacy questions could be addressed. Let us say that the first question is answered positively, in that the credit card purchasers might not know that the company has been "capturing" their names and addresses. The next thing to consider is whether the use of credit card numbers and purchases to form mailing lists violates any industry-specific statutes, such as the Fair Credit Reporting Act (1970). As this Act is now written, this type of use might be defined as a "legitimate business purpose" and, hence, violations of other laws (e.g., state laws about "capturing data on credit transactions") would have to be assessed.

If no violations were found of any types of privacy, technology control, consumer protection, or environmental protection laws, then the company would have to consider how comfortable it was with the ethics of its "capturing" activi-

ties. We can foresee some companies believing that by selling lists they were giving consumers more exposure to products they desired. However, other companies might find this behavior ethically indefensible because it does raise privacy issues.

Of course, companies might find themselves exploring different branches of this diagram depending on their competitive situations, the accuracy of information they use, and other factors. Our suspicion is that in the short run many marketers will find themselves exploring the privacy questions in the diagram. However, in the long run, as new privacy laws clarify what is permissible, we suspect managers will need to devote more attention to the questions about information exchanges, essential facilities, inaccurate information, consumer protection, and environmental protection. Determining where the boundary lines are on what is legal in some of these areas could be a substantial challenge, because new legal precedents and decisions are coming down all the time.

Research Needs

Scholarly research by marketing academics and others could be helpful in guiding public policymakers toward better approaches for dealing with some of the economic and social problems created by the use of new information technologies. Scholarly research also could help marketing practitioners find responses to legal and societal challenges. Research in areas such as the following could be helpful to public policymakers:

1. Descriptive research could be done on the pricing practices of the airline industry (or any other industries that use similar information systems to offer and publicize prices). Evidence of price signaling, parallel pricing, or other questionable behaviors could be sought by examining historical data.
2. Buyers of products or services in markets dominated by one or a few sellers could be surveyed or observed to determine how "essential" they find certain facilities controlled by these sellers (e.g., reservation systems, order-entry systems). Can the needs of the buyers be met readily by dealing with them through any other mechanism?
3. Descriptive research could be done on the frequency with which people are denied credit, insurance, or employment because of inaccuracies in credit reports or other data files. Factors that might influence the frequency of inaccuracies (e.g., the credit-reporting company, the type of person) also could be investigated.
4. Different ways of configuring rules for obtaining the permission of individuals to include their names in data bases could be examined. In particular, different approaches for presenting negative-option disclosures to consumers could be pretested and evaluated. This research could be similar in style to some of the work done on warning labels for cigarettes and alcohol (Andrews, Netemeyer, and Durvasula 1990; Fisher et al. 1989; Mazis, Morris, and Swasy 1991) and nutritional labeling (Levy 1992). Factors that could be considered include where the disclosures should appear (e.g., on invoices, envelopes, separate letters), how strongly worded they should be (i.e., should a fear appeal be used?), how often the wording should be changed (such as that done with cigarettes), and how large the type sizes should be.

Marketing managers and researchers could benefit from the following research:

1. Studies could be done of consumer attitudes toward industry self-regulation attempts. What do consumers think of codes of ethics or decisions to drop privacy-infringing products?
2. The conditions under which consumers can be deceived, misled, or confused when interacting with technologies could be examined.

Conclusion

As more marketers discover the power and benefits of using new information technologies to support their marketing programs, it is important for them to remember that use of these technologies can create legal and societal problems that they may not have seen before. Following the guidance we provide should help marketers reduce the chances that the use of new information technologies will lead to them being embroiled in costly litigation or targeted for protests by activist organizations. But the prudent marketer also should keep informed about how legal precedents and statutes are changing. Moreover, public opinion about these technologies should be monitored, because it shapes the laws and consumer responses facing the marketer. Keeping well informed about legal developments and public sentiment should allow most marketers to enjoy the benefits of new information technologies without experiencing surprising and costly challenges and attacks.

Appendix. Examples of New Information Technologies

This appendix provides examples of new information technologies that currently are used by marketers to improve (1) market knowledge, (2) response capabilities, (3) persuasive communications, and (4) strategy selection. When examining the subsequent discussion, note that technologies are placed under only one category (e.g., improving market knowledge). However, some technologies such as Caller ID can fit into more than one category (i.e., it can enhance market knowledge as well as improve response capabilities).

Market Knowledge

This includes technologies that can be used to obtain detailed information about customers, competitors, employees, and so on to enhance segmentation, targeting, product design, service features, promotion, and so forth.

- Computer matching—This typically occurs when a manager accesses several large data bases and matches data about an individual in one data base with information about him or her in other data bases. Usually the match is made on social security number because it is included on most documents and records pertaining to individuals. By combining data bases through matching, a more extensive profile of individuals is obtained and, in this way, the manager learns a great deal about an individual's shopping habits and personal characteristics—so that, ostensibly, better decisions can be made.
- People meters—This system monitors individuals to see if they are watching a particular television program. The sys-

tem verifies its audience through a camera device and matches the image with prerecorded images of family members. The individual's identity, time watched, and shows watched are then captured. This information is used to measure TV audiences.

- Smart cards—This device looks like a plastic credit card, but it also contains a tiny microchip that can store information. This technology, when used at the checkout counter, can pay for goods and record the customer's favorite items, recipes and personal details like birthdays and anniversaries. Marketers can use these devices for frequent shopping clubs, targeted data base mailings, and relationship building. The last benefit can be realized by other services such as quicker check approval, direct debit card functions, and a means for customers to have a conventional credit card. Also, cards could be preloaded to provide shoppers automatically with promotional offers.

Response Capabilities

This includes technologies that can be used to improve the accuracy and response times for order taking, bidding, delivery, and so forth.

- Caller ID (Sometimes known as Automatic Number Identification)—These systems allow the party who is receiving a telephone call to have the telephone number of the party who is calling displayed on a screen before the call is answered. Already introduced in several states, these systems have the potential of providing several benefits to their users. These include the usefulness of Caller ID in protecting individuals to screen and prevent harassing or obscene phone calls. Marketers also would benefit by improving their response times to customer inquiries. Faster access to a caller's telephone number should permit faster access to other information about the person stored in data files, which in turn should lead to faster responses to inquiries and orders. Knowing the phone numbers (and, perhaps, through the use of matching routines, the names) of people who have called also can prove valuable for companies interested in evaluating the impact of past promotional efforts or developing more effective targeted promotions in the future. Indeed, a list of names and phone numbers of people who have called about product X is something that marketers of other products might find extremely attractive. As a result, some marketers are using 800 and 900 numbers to capture callers' numbers and then match these numbers with names and addresses to build data bases for sale.
- Automatic order entry systems—These are systems in which sellers set up terminals and software to facilitate ordering by buyers. Automatic order entry systems are a valuable tool for many industrial marketers and can create great efficiencies for both sellers and buyers, reducing salesperson costs, inventory-carrying costs, and paperwork costs.

Persuasive Communications

This includes technologies that can be used to improve the efficiency and effectiveness of promotional approaches.

- Automatic dialers—These systems use computers to randomly dial the telephones. Then, once a number is reached, either a prerecorded message can be played, a fax can be sent, or a person such as a telemarketer or interviewer can respond. Newer systems, instead of randomly dialing phones, can screen for disconnected lines, busy signals, and no answers, and will only switch to the marketer when a live voice is on the line (as opposed to answering machines). Marketers gain efficiencies by minimizing the time telemarketers/interviewers must wait between calls, increasing the amount of time they can talk with clients, prospects, or respondents.
- Videocarts—This system, developed by IRI, transmits point of purchase information to a video screen attached to a shopping cart. The information shown on the video screen tells the customer what is on sale and where in the store it is located. The system starts with a commercial sent from IRI via satellite to a grocery store personal computer. Next, the commercial is transmitted by radio waves to the cart, and the ad can be viewed by the customer on the 6X9 inch screen that is mounted on the handle bars of the shopping cart. Marketers can communicate to customers by sending them an array of ads and coupon opportunities as they travel through the grocery store. The ads are transmitted to the screen when the customer moves near sending devices that can be spread out in different regions of the store. When a promotion is transmitted, the customer can select the coupon, and the computer on the cart stores the information and automatically transmits it to the cash register when the shopper enters a checkout line. The benefits to marketers are that point of purchase information can be sent to a purchaser in a more timely, active mode. Also, information on storewide purchases of videocart promotions versus other POP items could be tracked to help improve marketers' efficiencies.
- Videotext—This technology allows customers, through personal computers and modems, to access a wide range of information and assists them with their purchasing decisions. Marketers who sell their products through this channel get access to individuals who seek detailed information and want the convenience of shopping at home. By using videotext technology, which relies on the customers interactive involvement, persuasive sales messages can be sent to consumers who are already interested in buying from a product class.

Strategy Selection

This includes technologies that can be used to help marketers sort through information and select strategies and tactics that will be more efficient.

- Artificial intelligence or expert systems—These systems are interactive computer programs that allow marketers to solve problems, such as forming a negotiation strategy based on the accumulated expertise that is embedded in the program. NEGOTEX is an example of an expert system (Rangaswany et al. 1989). This system helps users to prepare for an ensuing international contract negotiation. There is potential for marketers to utilize expert system technology to help managers segment markets, prioritize sales calls, etc. Several marketing applications of expert systems already have been demonstrated: YCS's ADVISOR takes response to advertising and integrates the information into a general marketing model; IRI's SALESPARTNER gives marketer's account representatives evidence to present to buyers; COVER STORY, another IRI product, helps brand managers write memos and graphs (Winters 1991).
- Computer reservation systems—These systems are large-scale computer networks that the major airlines (e.g., American, United) use to transmit flight information to travel agents and, in turn, receive reservation information. Such a large computer based system provides tremendous efficiencies for the airlines, enabling them to select the most profitable combination of planes, routes, and seat availability. Airline carriers often use tactics referred to as "yield management," in which they attempt to maximize profits by offering cut-rate fares, but still mix the balance of low- and high-priced seats up until takeoff.

REFERENCES

American Column and Lumber Company v. U.S. (1921), 257 U.S. 377.

Andrews, J. Craig, Richard G. Netemeyer, and Srinivas Durvasula (1990), "Believability and Attitudes Toward Alcohol Warning Label Information: The Role of Persuasive Communications Theory," *Journal of Public Policy and Marketing*, 9, 1–15.

Antitrust & Trade Regulation Report (1991), "FTC and Federal Institutions Council Will Develop Joint FCRA Policy Statement," 60 (June 13), 821.

Areeda, Phillip E. and Herbert Hovenkamp (1989), *Antitrust Law: 1989 Supplement*. Boston: Little, Brown and Company.

Aspen Skiing v. Aspen Highlands (1985), 472 U.S. 585.

Associated Press v. U.S. (1945), 326 U.S. 1.

Birnbaum, Jeffrey H. (1991) "House Says 'Sorry, Wrong Number' to Telephone Sales," *Wall Street Journal* (November 19), B1.

Blattberg, Robert C. and John Deighton (1991) "Interactive Marketing: Exploring the Age of Addressability," *Sloan Management Review* (Fall), 5–14.

Bowers, Diane K. (1991), "The Privacy Challenge, Part I," *Marketing Research*, (June) 59–62.

Brockelesby v. United States (1985), 767 F. 2d 1288 (9th Cir. 1985), *cert. denied*, 106 S. Ct. 882 (1986), cited in Marx, 1988.

Brown v. United States (1984), 599 F. Supp. 877 (D. Mass. 1984), cited in Marx, 1988.

Buzzell, Robert D. (1985), *Marketing in an Electronic Age*. Boston: Harvard Business School Press.

Cable Communications Policy Act of 1984, 47 U.S.C. § 551 et. seq.

California H.B. 1446, Ch. 483.

Caller ID Technology Hearing (1990), Y4.J89/2:S.hrg.101-1264.

Carnevale, Mary Lu (1992), "FCC Adopts Rules to Curb Telemarketing," *Wall Street Journal* (September 18), B1.

———— (1993), "Telemarketers Fight Banning of Autodialers," *Wall Street Journal* (January 20), B1.

Cauley, Leslie (1993), "Steve Jobs: Cut Microsoft in Half," *USA Today* (February 11), 2B.

Chain Store Age Executive (1991), "Quick Response: What It Is; What It's Not," (March), 4B–17B.

Computer Matching and Privacy Act of 1988, 5 U.S.C. §552a *et. seq.*

Consolidated Gas v. City Gas (1987), 665 F.Supp. 1493 (S.D. Fla.).

Consumer Reports News Digest (1992), "President Bush Signs Bill Guarding Against Unwanted Phone Calls," 17 (March), 12.

Consumers Union (1991), "What Price Privacy?" *Consumer Reports*, 56 (May), 356.

Culnan, Mary J. (1992), "How Did They Get My Name?: An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use," working paper, School of Business Administration, Georgetown University.

Dahl, Jonathan (1991), "Agents Rankle Airlines with Fare-Checking Programs," *Wall Street Journal* (May 20), B1.

Davidson, Joe and G. Pascal Zachary (1993), "FTC to Hold Feb. 5 Meeting on Microsoft," *Wall Street Journal* (January 8), A3.

di Talamo (1991), "Private Secrets," *Direct Marketing* (April), 42–44.

Direct Marketing Association (1990a) *DMA Government Affairs Compendium Update* (January 1, 1990–April 30, 1990).

———— (1990b), *Telemarketer's Guide to State Laws*.

Dun and Bradstreet v. Greenmoss Builders (1985), 105 U.S. 2939.

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

Fair Credit Reporting Act (1970), 15 U.S.C. 1681-1681t.

Farhi, Paul (1989), "Some Machines Won't Take No For an Answer," *Washington Post National Weekly Magazine* (October 16–22), 34 at col. 4.

Fisher, Paul M., John W. Richards, Jr., Earl J. Berman, and Dean M. Krugman (1989), "Recall and Eye Tracking Study of Adolescents Viewing Tobacco Advertisements," *Journal of the American Medical Association*, 261 (January 6), 84–89.

Geyelin, Milo and Mary Lu Carnevale (1992), "Caller ID Service Is Ruled Illegal in Pennsylvania," *Wall Street Journal* (March 20, 1992), B1.

Givens, Richard A. (1989), *Antitrust: An Economic Approach*. New York: Law Journals Seminars-Press.

Glazer, Rashi H. (1991), "Marketing in Information-Intensive Environments: Strategic Implications of Knowledge as an Asset," *Journal of Marketing*, 55 (October), 1–19.

Guerin-Calvert, Margaret E. (1989), "Vertical Integration as a Threat to Competition: Airline Computer Reservation Systems," in *The Antitrust Revolution*, John E. Kwoka and Lawrence J. White, eds. Glenview, IL: Scott, Foresman & Co, 338–70.

Harvard Law Review (1990), "The Legal and Regulatory Implications of Airline Computer Reservation Systems," 103 (June), 1930–50.

Herring, Phil (1992), "Life Beyond the Spreadsheet," *Direct Marketing* (February), 49–51.

Honomichl, Jack (1992), "Industry Seeks Support for $500,000 Lobbying Effort," *Marketing News* (March 2, 1992), 9.

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

Hylton, Keith N. (1991), "Economic Rents and Essential Facilities," *Brigham Young University Law Review*, 191 (3), 1243–89.

Ingrassia, Lawrence (1992), "Judge Says MIT Broke Antitrust Laws by Sharing Financial Aid Information," *Wall Street Journal* (September 3), A4.

In re Domestic Air Transportation Antitrust Litigation (1990), DC NGa, No. 1:90-CV-2485-MHS, MDL No. 861.

Levy, Alan S. (1992), "An Experimental Study of Food Label Formats," completed by the Food and Drug Administration and presented at the 1992 Marketing and Public Policy Conference, Washington, DC (May 15).

Marketing News (1990), "Environmentalists Give Nod to Some Direct Mail" (December 10), 7.

Marx, Peter (1988), "The Legal Risks of Using Information as a Competitive Weapon," *Software Law Journal*, 2, 185–201.

Maryland Commercial Law, Section 13-317. Use of consumer identification in connection with credit card payments.

————, Section 13-318. Use of credit card information in connection with payment by check.

Mazis, Michael B., Louis A. Morris, and John L. Swasy (1991), "An Evaluation of the Alcohol Warning Label: Initial Survey Results," *Journal of Public Policy and Marketing*, 10 (1), 229–41.

MCI Communications v. AT&T (1983) 708 F. 2d 1081 (7th Cir.), *cert. denied*, 464 U.S. 891.

Menell, Peter S. (1987), "Tailoring Legal Protection for Computer Software," *Stanford Law Review*, 39 (July), 1329–72.

Miller, Cyndee (1989), "Telemarketing Foes: Don't Reach Out to Us," *Marketing News*, 23 (July 3), 1,14.

Miller, Michael W. (1990), "Coming Soon to Your Local Video Store: Big Brother," *Wall Street Journal* (December 26), 12.

———— (1991a), "Six States Sue TRW Over Credit-Reporting Practices," *Wall Street Journal* (July 10), B1.

———— (1991b), "Lotus is Likely to Abandon Consumer Data

Project," *Wall Street Journal* (January 23), B1.
——— (1991c), "'Greens' Add to Junk Mail Mountain," *Wall Street Journal* (May 13), B1.
——— (1992), "Patients' Records Are Treasure Trove For Budding Industry," *Wall Street Journal* (February 27), A1.
Nomani, Asra Q. (1991a), "TWA Settles Price-Fixing Suit, Meaning Sweeter Deals for Passengers Involved," *Wall Street Journal* (June 20), A4.
——— (1991b), "NWA, TWA Agree to Alter Pricing Actions," *Wall Street Journal* (June 21), B1.
O'Callaghan, Ramon, Patrick J. Kaufmann, and Benn R. Konsynski (1992), "Adoption Correlates and Share Effects of Electronic Data Interchange Systems in Marketing Channels," *Journal of Marketing*, 56 (April), 45–56.
Otter Tail Power v. U.S. (1973), 410 U.S. 366.
Peck, Robert S. (1984), "Extending the Constitutional Right to Privacy in the New Technological Age," *Hofstra Law Review*, 12 (Summer), 893–912.
Podell, David M. (1989), "The Evolution of the Essential Facilities Doctrine and its Application to the Deregulation of the Natural Gas Industry," *Tulsa Law Journal*, 24, 605–25.
Privacy Act of 1974, 5 U.S.C. § 552a *et. seq.*
Pulley, Brett and Bridget O'Brian (1992), "More Airlines to Settle Suit on Price-Fixing," *Wall Street Journal* (June 23), A3.
Radding, Alan (1991), "Consumers Worry Halts Data Bases," *Advertising Age* (February 11), 28.
Rangaswamy, Arvind, Jehoshua Eliashberg, Raymond R. Burke, and Jerry Wind (1989), "Developing Marketing Expert Systems: An Application to International Negotiations," *Journal of Marketing*, 53 (October), 24–39.
Rebello, Kathy (1993), "Is Microsoft Too Powerful?" *Business Week* (March 1), 82–90.
Right to Financial Privacy Act of 1978, 12 U.S.C. § 1341 *et. seq.*
Rothfeder, Jeffrey (1992), *Privacy for Sale*. New York: Simon and Schuster.
Salop, Steven C. (1986), "Practices that (Credibly) Facilitate Oligopoly Co-ordination," in *New Developments in the Analysis of Market Structure*, Joseph E. Stiglitz and G. Frank Mathewson, eds. Cambridge, MA: MIT Press, 265–94.
Sanchez, Jesus (1992), "Airline Lawsuit Won't Mean Quick Benefits for Consumers," *Raleigh News and Observer* (December 27), F1.
Simitis, Spiros (1987), "Reviewing Privacy in an Information Society," *University of Pennsylvania Law Review*, 135 (March), 707–46.
Smith, Glenn Chatmass (1989), "We've Got Your Number! (Is It Constitutional to Give It Out?): Caller Identification Technology and the Right to Informational Privacy," *UCLA Law Review*, 37 (13), 145–223.
Stacey, Robert T. (1992), "Canada's Push for Privacy Legislation," *Direct Marketing* (March), 57.
Stern, Louis W. and Thomas L. Eovaldi (1984), *Legal Aspects of Marketing Strategy: Antitrust and Consumer Protection Issues*. Englewood Cliffs, NJ: Prentice-Hall, Inc.
Texas v. TRW, Inc. (1991), Texas DistCt (Dallas), No. 91-07999, 7/8/91.
TRW, Inc. v. Texas (1991), DC NTexas, No. CA3-91-1340 H, 7/8/91.
United Airlines et al. v. Civil Aeronautics Board (1985), 776 F.2d 1107, 1109 (7th Cir., petition denied).
U.S. v. Brown University et al. (1991), DC E PA, May.
U.S. v. Container Corporation of America (1969), 399 U.S. 333.
U.S. v. Terminal Railroad Assn. (1912), 224 U.S. 383.
U.S. v. United States Gypsum Co. (1978), 43 U.S. 422.
Video Privacy Protection Act (1988), 18 U.S.C. § 2710 *et. seq.*
Wilke, John R. (1991), "Lotus Product Spurs Fears About Privacy," *Wall Street Journal* (January 15), B1, B5.
Wilcox, Clair (1971), *Public Policy Toward Business*. Homewood, IL: Richard D. Irwin, Inc.
Winters, Lewis C. (1991), "Artificial Intelligence and Expert Systems in Marketing," *Marketing Research*, 3 (March), 72–74.