Top of Form

|  |
| --- |
| Abstract Article:  ABSTRACT. Individualized customer information is at the heart of on-line commerce. Using increasing amounts of customer-specific data enhances the success and value of one-to-one on-line marketing; but the extensive gathering and use of data specific to individuals also causes alarm over the loss of digital privacy, setting up a confrontation between ecommerce and society. Governments and nations, particularly in Europe, have reacted with a reliance on sweeping laws governing digital privacy protection while other nations such as the U.S. have generally preferred to allow companies and industry associations to regulate themselves. This tenuous balance is under attack from both sides. In this paper, we set up a framework which incorporates the environmental context, ethical perspectives and firm-specific considerations to help firms develop a strategy for handling digital privacy concerns. |

|  |
| --- |
|  |

Travelers facing interminable queues at airports and needing to arrive at the airport hours ahead of their flights for security inspections might welcome ethnic profiling, even though it means a loss of privacy, if it also reduces the waiting and lost time at airports. Fears of terrorism have led several U.S. politicians and legislators to propose national ID cards, a development opposed by civil libertarians such as the American Civil Liberties Union. Here the loss of privacy is being balanced against possible gains in personal security.

In the commercial arena, pharmaceutical firms attempting to increase the sales of their products have sought to dislodge their rivals by obtaining data from pharmacies about customers to whom such rival drugs have been sold, and then using the information to prepare personalized marketing communications offering customers their own pharmaceuticals as a replacement for their current prescription, sometimes in different but more convenient dosages (weekly rather than daily) and at higher prices. Lost in this marketing shuffle is the invasion of individual medical privacy. Landlords might deny rentals to tenants based on less than satisfactory credit reports, with the would-be renter unaware of the reasons for denial of the rental. Record club companies, like many other consumer product companies, use past purchase histories to infer musical preferences of their members, and then send personalized e-mail messages to each member, offering sale prices on products likely to be of interest to each individual customer. Each offer is different and tailored to the individual customer, costs pennies to compose and send, and the ROI to the firm can be very high, as the conversion rate, of individuals responding to the offer to buy, is quite attractive.

The above examples illustrate two kinds of privacy concerns: individual privacy vs societal good (anti-terrorism, for example); and, individual privacy vs. commercial interests - i.e. better marketing, increased sales. If broad societal concerns lead to some toleration of erosion of privacy, can similar acceptance or toleration be expected in e-commerce transactions? While companies increasingly seek greater customerspecific information in the interests of efficient and effective marketing, customer activists and governments are in turn seeking to regulate such data gathering and use. Should corporations fight back to protect their ability to invade privacy, or, analyze societal and national trends, and cooperate with customers and governments in accepting some limits on their invasion of customer privacy? How can ethical frameworks inform companies as they develop their privacy protection strategies? Should companies accept some regulation of data privacy as inevitable and work to frame laws that protect both customer and commercial interests? This paper examines the issue of data privacy in commercial contexts and develops a framework that can help companies develop a data privacy protection strategy. There have been several recent efforts to apply ethical frameworks in tackling the privacy problem (i.e. Caudill and Murphy, 2000; Charters, 2002; Sama and Shoaf, 2002); however, most of these analyses focus principally on ethics, and we seek to incorporate ethics along with other contextual and firm-level factors in developing a strategic approach to privacy.

Lessig (1999) asserts that the Internet poses fundamental challenges to issues central to society, namely free speech, privacy and national sovereignty. As Kelly and Rowland (2000, p. 2) note, "the advent of electronic commerce brings with it a host of ethical issues surrounding customer privacy." Eisenberg (1996) sees the topic of protecting individual and corporate privacy as a major ethical issue which has triggered a wave of governmental legislation and has created an entire segment of Internet industry firms whose mission is to help consumers protect sensitive and personal data on the web, for instance, by becoming anonymous as they visit web sites (Introna and Pouloudi, 1999).

The backlash against corporate use of individualized data for marketing purposes is widespread. A number of lawsuits filed recently have alleged that dominant Internet advertising firms have gone too far in their quest to develop highly individualized information on which to base Internet marketing efforts (Griffith and Palmer, 1999). One prominent example is the case of DoubleClick, Inc (Charters, 2002). DoubleClick, a leading Web advertising firms, inserts banner ads and promotional messages on thousands of Web sites. In order to better direct messages at their respective target audiences, DoubleClick tracks Web surfer buying patterns by storing small files on users' computers, known as "cookies", which identify these individuals as they browse web sites. Knowledge of each individual's web surfing behavior, coupled with detailed individual data, such as their purchasing history, age, income, and address, allows for highly personalized targeted marketing. This linking of on-line surfing behavior with real world marketing demographic information was made possible when DoubleClick purchased Abacus Direct Corporation, a catalog direct marketer of long standing with detailed databases containing purchasing histories of millions of consumers. Many individuals and public interest organizations see such gathering of information on vast numbers of individuals as a troubling invasion of privacy and are banding together to stop such corporate actions. These concerns led to a 10state 30 month inquiry led by New York state, culminating in DoubleClick agreeing to make its tracking of consumers more visible and giving consumers access to their online profiles, as well as paying the states $450,000 for investigative costs and consumer education. It also settled a related consolidated class action with a payment of $1.8 million in attorney fees and agreed with the FTC not to use personally identifiable information in its online tracking (Computer and Internet Lawyer, 2002; Journal of Internet Law, 2002; Hemphill, 2001).

The purpose of this paper is to help firms incorporate both ethical and firm-specific perspectives in developing a strategy for customer privacy protection in their e-commerce activities. To help achieve this goal, we have developed a model of "Factors Influencing Privacy Strategy." We focus on several dimensions that influence how a firm develops, consciously or tacitly, a privacy protection strategy: the firm's national historical and cultural context, the legal environment, and its ethical philosophy. We also discuss firm-specific factors that affect a firm's privacy posture, including the firm's line of business and its corporate culture. These influences, moderated by a cost-benefit filter, suggest a privacy strategy for the firm positioned on a continuum between self-regulation and governmental regulation. We then use an example to show how a firm, under certain assumptions, might develop privacy protection strategies for a variety of situations.

A model of factors influencing privacy strategy

Precursors

Figure 1 presents a model of factors influencing a firm's privacy strategy. The model commences by positing that external uncontrollable factors, consisting of national history and culture, global societal trends in privacy protection, extant and projected legislation and the importance and sensitivity of data being gathered provide a context for situating the privacy strategy decision.

National history and culture. Cultures may stress the individual or the collectivity. This balance can change over time and the rise of democracy in many countries has been accompanied by an increase in the primacy of individual rights. However, not all countries subscribe to the notion of privacy as a fundamental human right, which colors the way a nation accepts the need to protect individual privacy rights. Thus "democracies may converge on a basic set of principles for data protection or data privacy, (and) these norms of fair information practice constitute what can be termed First principles, and their acceptance separates democratic societies from totalitarian regimes" (Reidenberg, 2000). The socioeconomic environment of a nation also plays an influential role in shaping choice for a variety of organizational issues, such as human resource policies and marketing strategies (Shane and Venkataraman, 1996). Cultural factors such as religion, kinship, and individual vs. group-orientation weigh in the determination of a society's beliefs about protecting individual privacy (Donaldson and Werhane, 1996). A nation's history can provide clues to its preferences concerning respect for an individual's privacy. Furthermore, the business context, the extent to which a nation's economy is market driven, drives privacy views.

Global societal trends also influence the state and perception of privacy. After the events of September 11, 2001 U.S. citizens have been more willing to sacrifice some of their privacy to help promote a more safe and secure environment. This is particularly true with the heightened security at airports and border crossings. The political shift in Eastern Europe over the past decade away from Communism has also resulted in a change in privacy beliefs. As democratic nation states have become more prevalent people tend to be less open to government intrusion into their private lives (Ger and Belk, 1996).

Together, these national, cultural and societal influences create a predisposition as to how privacy should be respected and treated in a given country. For example, the European Union's emphasis on Europe-wide governmental regulation over protecting consumer data privacy may be interpreted as a reaction to the excesses of various oppressive regimes in the earlier part of the twentieth century and the continuing fear of the misuse of personal data by corporate and government entities. Whereas U.S. approaches, rooted in a history of entrepreneurial behavior and laizzez-faire capitalism, have leaned towards industry self-regulation, preferring that firms and their customers negotiate levels of privacy protection that are acceptable to both sides.

External factors

Existing and pending legislation. Companies seeking long-term survival and prosperity will seek to comply with the letter of the law if not exceed it in spirit. For most companies, existing and pending legislation will provide a floor above which firms will develop policies for data privacy strategies. The impact of legislation and lawsuits can be seen in the fact that companies as prominent as Microsoft and Eli Lilly have settled lawsuits over privacy matters. Microsoft settled with the FTC over charges that it misrepresented its information practices and privacy protection in connection with its Passport Web services (Computer and Internet Lawyer, Oct. 2002). Eli Lilly settled with the New York Attorney general over charges that it infringed on the privacy of its consumers by allowing 670 email addresses to be visible in a Prozac related mass emailing (Computer and Internet Lawyer, Nov. 2002). And because of the passage of HIPAA (Health Insurance Portability and Accountability Act) healthcare companies ranging from hospitals, to Strategic and Ethical Considerations in Managing Digital insurance companies, HMOs, and individual doctors have to implement a range of practices to protect medical privacy (Tang, 2000).

U.S. legislation governing privacy protection has been piece-meal and industry specific, creating different standards for different industries as well as a disparity in regulations between the public and private sector (Samuelson, 1999). A variety of Federal laws govern privacy, such as the Telecommunications Act, the Cable Communications Policy Act, the Fair Credit Reporting Act and others, with an emphasis on the safeguarding of data on consumers gathered by telecom companies, cable TV companies, credit report bureaus and the federal government. More recently, consumer alarm over the gathering and use of data on the Internet has led to specific industry focused legislation (Robertson and Sarathy, 2002) such as:

\* the Children's On-Line Privacy Protection Act, which requires companies operating web sites focusing on children to seek parental consent to data gathering and requires the use of comprehensive privacy policies;

\* the Financial Modernization Act ("GrammLeach-Bilkey" act) which addresses financial institution and place disclosure requirements and restraints on the transfer of financial information on consumers within the company and to non-affiliated third parties; and

\* the Electronic Signatures Act which creates a framework for binding electronic signatures, thus affecting electronic contracts and privacy issues surrounding such contracts;

However, these various acts are still discrete attempts at regulating specific privacy areas and are a reactive response to consumer concerns, quite different from the Europe-wide Data Privacy Directive which is rooted in the legal protection of privacy as a fundamental human right (George et al., 2001; Fromholz, 2000).

Importance and Sensitivity of Data being gathered. Individuals do not have the same concern about all data pertaining to themselves. Individuals have different preferences for privacy for different kinds of data and depending on the context in which this data is disclosed. For example, individuals may be less willing to disclose data on political and sexual preferences, health related information and financial information, than on their current consumption preferences and likes and dislikes in entertainment; and for more sensitive data such as health information, they may be more willing to share such data with their medical care-givers, less so with insurance companies and even less so with banks and pharmaceutical companies. Some data is permanent and can identify individuals, i.e. name, age, address, and individuals may be quite protective of such data; other data is transitory and can change i.e. tastes in clothes, movies, books etc., and individuals may care less about sharing such data. People may be quite willing to share less sensitive data and transitory data for a consideration, i.e. if they are compensated for sharing such information. In this context, Blanchette and Johnson (2002) discuss the issue of social forgetfulness in three areas - bankruptcy, juvenile crime and credit reports, pointing out that such data are more sensitive and the creation of databases where such information are stored permanently make it difficult to give individuals a "second chance"; they make pleas for timely disposal of sensitive data from databases as a way of protecting privacy in the long-term.

Ethical frame

While external factors such as culture, business context, legislation, nature of data and history all play a role in shaping a firm's privacy strategy, the implicit and explicit ethical ideology of the firm, its founders, and top management team, establish a moral dimension to the chosen privacy strategies (DeGeorge, 2000). While other researchers have elected to develop models that identify the various steps in the ethical decisionmaking process (i.e. Jones, 1991; Trevino, 1986), we have incorporated the concept of moral philosophy into our model (Fritzsche and Becker, 1984). There are four categories of ethical theories that are relevant to managerial behavior in the current context, Utilitarianism, Egoism, Moral Relativism, and Justice (Boatright, 1999; Cavanagh et al., 1981). Each theory is grounded in a moral ideology that stresses an individual's role in the ethical decision-making process and an exploration of this phenomenon can be particularly useful "in understanding the values held by managers as well as in providing a basis for altering behavior in a more ethical direction if such a change is deemed to be in the best interests of society" (Fritzsche and Becker, 1984, p. 166). The amalgamation of a firm's dominant moral philosophy generally constitutes the soul of a firm's corporate culture. Thus, an analysis of the various influences on privacy stances without considering the moral perspective of the individual and the firm would ignore one of the fundamental drivers of ethical decision-making (Boatright, 1999). Moreover, injecting moral philosophy into the privacy debate provides an additional lens from which to view this issue. Each theory will be discussed in terms of its relevance to digital privacy issues.

Utilitarian theories tend to fall into two categories, rule or act utilitarianism (Premeaux and Mondy, 1993). With rule utilitarianism each decision is evaluated based on any relevant rules or laws. The genesis for rule utilitarianism rests in the belief that in the long run the following of rules will lead to the greatest societal benefit (Barry, 1979). An act utilitarian approach results when one bases a decision on its consequences and the act resulting in the greatest good is selected. Here, the results are paramount and trump any harm created by the explicit actions involved. The underlying premise of utilitarianism is that individuals should evaluate decisions in terms of their impact on society. From a privacy perspective, a firm that follows an act utilitarian approach would weigh the consequences of greater respect for privacy (and the trade-off of profitability and job creation versus individual privacy rights). A firm following a rule utilitarian mindset would stress consumer benefit and prefer to behave in a legally compliant manner. For example, a marketing research firm following utilitarianism would decide how much privacy protection they would abide by, weighing the invasion of personal privacy, such as the procurement of religious or sexual preference information, against potential benefits which might include providing better services to customers and job creation through increased corporate revenues and profits.

Egoism is an ethical philosophy in which individuals, or firms, justify their actions based on their own self-interests. According to Ferrell et al. (2000, p. 54) egoists "do the act that promotes the greatest good for oneself." Thus for profit firms might place profit maximization above other goals. Such a firm that happens to sell pharmaceutical products might therefore attempt to procure as much individual medical information as is legally possible, to maximize sales and eventual profits. The egoist approach is grounded in the definition of ethicality in subjective terms (Epicurus, 1963) and as long as an action is legal, such as tracking on-line buyer behavior, decisions will be made based on the firm's paramount goals.

The moral growth of individuals who are involved with making strategic decisions about privacy issues is also a factor influencing where the firms end up in making privacy protection decisions. As Kohlberg's (1984) stages of moral development have shown, individuals tend to operate in different levels, or stages, of moral rationalization. Whether a manager is trying to avoid punishment, obey laws as a good duty to society, or assert personal idealistic beliefs, this variance in cognitive moral reflection can influence the ultimate privacy strategy chosen by the firm.

The notion of Moral Relativism refers to defining ethical behavior in the context of individual and group norms (Ferrell et al., 2000). A moral relativist surveys colleagues and industry competitors, formally or informally, to determine a range of generally accepted standards of behavior for specific issues. Essentially, moral relativism implies perceived moral acceptability and the individual and the firm adopt behavior which conforms to the norms noted for the industry or reference group. Ethical stances on various issues may vary over time as the reference groups chosen for comparison change, and as the behavior of the groups themselves change over time. Legal and public perceptions influencing the relativist stances of firms. For example, the public campaign against the use of sweatshops in developing countries has resulted in a shift in standards in the footwear industry by firms such as Nike and Reebok. In a sense, the moral judgment of others is substituted for one's own moral judgment. Following this theory, a mortgage company might sell information on its customers' debt and finances to an independent insurance company if this was the prevailing industry standard, and not concern itself much with whether its customers should be consulted. Relativism, through its method of referencing others' moral beliefs as a decision-making basis, tends to imply that legality carries more weight when making a moral decision. Laws and regulations can certainly be viewed as an ethical reference point.

The idea of justice has been debated by philosophers for centuries. In modern times, the notion of justice has arguably been best articulated by John Rawls in his book Theory of Justice (1971). In business ethics, justice is determined on the basis of fairness and any accompanying perceived injustices (Ferrell et al., 2000). Rawls' theory focused on the idea of social justice, which is essentially the determination of what constitutes a just society. Questions of justice also stem from when individuals attempt to advance their personal interests and their objectives clash with other individuals attempting to maximize different personal goals (Rawls, 1971). Three types of justice are generally examined; distributive justice, which is based on the evaluation of outcomes or results of the business relationship; procedural justice, based on the processes and activities that produce the outcomes or results; and interactional justice, the evaluation of the communication process used in the business relationship (Ferrell et al., 2000).

Firm-specific factors

Although the legal and ethical dimensions of privacy protection have a major impact on privacy strategy decisions, firm-specific factors also play a significant role in this process.

Information intensity of business. The nature of a firm's business can determine the degree of its privacy protection. While traditional manufacturingbased, or product-driven, firms are still dominant in much of the economy, the rapid growth of e-commerce in the last few years has created an entirely new type of virtual, information-driven, business, sometimes termed as infomediaries. Information-based firms are principally services businesses, and often play the role of intermediaries or matchmakers, matching firms with their potential customers. These firms tend to be more externally and consumeroriented. Compared to manufacturing-based firms, infomediaries are more likely to gather greater amounts of personalized information and use it as a fundamental differentiating element in their business strategy. However this distinction is likely to diminish as more old economy "brick and mortar" firms use e-commerce as a channel of distribution in their industries. However, as personalization and customer information become increasingly important in a firm's marketing strategies, privacy protection will become a discriminating factor. As more firms rely increasingly on individualized customer information to achieve marketing success, they will seek flexibility and speed of response in using such data. Under these circumstances firms might well prefer self-regulation as a means of preserving their edge in fast-changing environments, rather than concur with government-set privacy regulations. If government standards have to be met, they might prefer a level playing field with clearly established standards applied uniformly to all companies.

Profit/Non-Profit orientation of the firm. The profit vs. nonprofit nature of the organization clearly has an impact on the firm's privacy philosophy. A firm unmotivated by profit may be less interested in pursuing marketing approaches that intrude on consumer privacy. However, even non-profit firms, such as non-profit hospitals, will come under the purview of privacy considerations, as they struggle with the need to provide better service while being respectful of patient privacy. As noted earlier, the passage of HIPAA has forced all non-profit as well as for profit medical establishments to grapple with stringent privacy regulations as they affect medical data.

Ownership: private, publicly-held, state-owned. Publicly-held companies may face greater pressure to put profits ahead of individual privacy rights; this pressure may stem from the perception that enhancing shareholder value is linked to current profits, and from managers holding stock options who seek to maximize stock option values. Private firms because they are not subject to stock market pressures (they are family owned or closely held) may be more diligent about ensuring customer loyalty in the long-run, a goal which might be furthered by giving greater privacy protection. Of course, maximizing shareholder wealth can lead to more greed as well in the private sector.

State-owned firms may face a different context in that people may be more trusting of Government firms and have fewer qualms about sharing data with state-owned firms. State-owned firms may also have access to information obtained through multiple avenues and the difficulty here may lie in deciding how much information should be combined together from diverse sources in fulfilling customer needs. Stateowned firms may also place a lower priority on enhancing customer satisfaction, particularly when customers are captive, such as in stateowned water and energy utilities. Under these circumstances, state-owned firms may have little interest in gathering information on the customer and may have to be encouraged to obtain such information so as to enhance the quality of the service they provide.

Age and experience of the firm (particularly with e-commerce). The age of a firm can also mediate privacy protection preferences. New firms that have adopted e-commerce as the sole or principal channel of distribution may be less careful of individual privacy protection, while established mass market consumer firms may be more sensitive to maintaining the long-term loyalty of consumers and avoid actions that anger current customers. As e-commerce increases in importance, the firm's business becomes more informationintensive, raising the importance of developing effective data privacy policies. Learning from experience will be important. This entails keeping track of a firm's interaction with its customers over data privacy issues, and performing regular "lessons learned" de-briefings, modifying privacy protection policies continually as customer provide feedback on their privacy preferences. One might hypothesize that as customers become more comfortable with a firm and with sharing data with the firm, their privacy protection concerns might decrease.

Industry best practices (and current data privacy protection policies). Given that privacy protection is a relatively new concern for both firms and their customers, most firms might at the outset follow the industry leaders, the e-commerce pioneers. In the spirit of continual improvement, observing and imitating industry and competitor best practices will help the firm enhance its privacy protection policies and its trustworthiness in the eyes of its customers. Competitive dynamics also suggest that firms feel the necessity to adhere to competitive and industry best practices.

Corporate culture and the top management team's ethical perspective. Both of these factors tend to reflect the mission, objectives, and values of the firm, its founders, and its top management team, their overall willingness to accord high importance to the issue of privacy protection. The ethical perspectives of the top management team determine whether the firm will be proactive and a leader in setting privacy protection policies, whether privacy protection is put ahead of profits. A corporate culture that is customer oriented will ask customers about their privacy protection needs and listen to the fears of customers regarding the erosion of their privacy. Such conversations will lead the firm to treat privacy protection as a long-term goal and value, setting a high bar for competitors and the industry.

Table I sets out the potential impact of these several factors on the privacy strategy likely to be adopted by a firm.

Cost-benefit analysis filter

How a firm resolves its privacy strategy will also be affected by a cost benefit analysis. Simply put, the firm may choose to weigh the revenue gains and customer goodwill to be had from adopting different privacy strategies against the cost of compliance imposed by differing privacy strategies. These results will be assessed against the ethical position adopted by the firm, with the strongest decisions being those that provide positive cost benefit and are consistent with the firm's ethical stance.

Whether the firm is following a utilitarian, egoist, justice-based or relativist ethical frame determines how much priority is given to the cost-benefit filter. Egoist firms may place the highest reliance on the results of the cost-benefit analysis, with the privacy strategy chosen that gives the largest cost-benefit (It should be noted that the idea of a cost-benefit filter is arguably an egoist concept although there are surely implications for the other theories as well). A relativist firm might choose a strategy that is consistent with the majority of the industry and yields a positive cost-benefit. An utilitarian firm might view positive cost-benefit as a desirable secondary outcome. From a justice perspective the balancing of fairness to all involved stakeholders would be paramount. We may hypothesize that greater privacy protection may result in increased traffic to the site, possibly resulting in increased revenues; however, this may also result in less effective personalization of the marketing function. On the cost side, higher cost would result, with cost drivers including:

\* the costs of granting access to data gathered on each consumer

\* costs of providing notice of privacy policies

\* the costs of obtaining individual consent

\* the costs of creating greater transparency and

\* the costs of granting customers choice including that of opting out or opting in to the database.

As market pressures impinge on publicly owned firms, the drive to enhance revenues and profits may push such firms to reduce the privacy protection extended to customers, with the intention of raising short-term revenues and lowering short-term costs. However, such behavior could lead to customer defections in the medium to long-term as customers unhappy over the reduced privacy protection seek supply alternatives. Firms may rationalize the lowering of privacy protection by pointing to the possibilities of increased marketing personalization, contending that such customized marketing enhances customer satisfaction. This suggests that customers may be willing to sacrifice their privacy in return for some level of payoffs and this raises the possibility that customer privacy protection is not an absolute target; instead, firms may have an additional option of relying on market prices, and buying information from the consumer: they can offer a payment in cash or in kind (the promise of personalization, of price discounts, of increased customer satisfaction), in exchange for the surrender of more personal information (Bibas, 1994). Such a policy would fit in well with a U.S. company predilection for self-regulation.

Implementation. Working through these various factors results in a firm's eventual privacy strategy. The basic choice is between self-regulation, the current U.S. choice, and government regulation, the practice in the European Union, and one which is gaining greater support in the U.S. (Green, 2000), as evidenced by the increasing flow of legislation described earlier. More fundamental is the impact of the privacy strategy on gaining consumer trust; it is the lack of trust that causes consumer anxiety over loss of privacy. A corollary is that as firms prove themselves worthy of trust, customers may voluntarily provide more data about themselves, suggesting that strong privacy protection can enhance customer data availability - a virtuous cycle!

Another variable affecting a firm's privacy strategy is the audit mechanism, designed to validate compliance with stated privacy principles and to disclose performance relative to stated privacy standards, which would serve to increase consumer trust and foment better long-term customer relationships. However, the mere existence of sanctions is insufficient, as firms may well choose to not comply with regulations or industry practices and accept sanctions, if they are seen as mild and as a cost of doing business. Such behavior would only increase consumer mistrust. Strong sanctions and their rigorous use are necessary to convince clients that stated privacy policies are being implemented, this being a necessary step to greater trust down the road. It is worth adding that we are assuming that firms behave rationally. Strategic choices affecting privacy may also be subject to pressures faced by corporate leaders, individual biases of key managers and the resolution of interorganizational conflict over privacy.

Discussion

Figure 1 and Table I provide a framework that incorporates several variables that influence the development of a firm's privacy strategy. How can a firm use the framework in Figure 1 to develop its privacy protection strategies? We apply this framework to an illustrative U.S. firm, whose context is a corporate culture that is strongly profit-oriented, is a large publicly-held firm, and is a relative newcomer to e-commerce. How might such a firm react when faced with a variety of digital privacy issues? The issues are as described below:

(a) the human resources department of a large multinational seeks information on sexual preferences of its employees as part of its efforts to develop a diverse workforce, and to document such efforts in a database that would then be used in its "cafeteria-style" benefits programs;

(b) a pharmaceutical firm obtains drug prescription data from pharmacies and then uses such information to have the pharmacy send out letters to customers offering them the choice of switching to a competing drug offered by the pharmaceutical company;

(c) a record club company develops a database of customer musical preferences based on purchase histories and then send e-mail sales pitches offering discounts on new CDs and tickets to musical concerts;

In Table II the three scenarios outlined above are matched against the ethical frame that we discussed earlier. Based on the scenario and the ethical frame that a firm follows a number of plausible privacy strategies exist. In the first scenario, seeking to procure sexual preference information, a utilitarian approach would likely lead a firm to permit individuals to opt out of providing information based on existing laws and the potential benefits to society for such a program. In this situation the egoist firm would try to maximize its self-interests, wealth maximization, and would pursue the sexual preference information if it supported this goal. A firm following a relativist approach would assess industry norms and follow the practice that is commonplace. A firm emphasizing justice would be concerned with fairness and attempt to educate employees about why the information is being sought while being accepting of employees whose choice is to not provide such information. The significance of the sexual preference information to firm goals, and the public versus private nature of this firm, are clearly relevant to any final decisions.

In the prescription drug example a utilitarian stance would probably yield a decision to offer a fee or discount to the customer for the personal medical information. Again, local laws and overall consequential benefits (such as customers receiving drugs at lower prices) are emphasized. The egoist stance would result in a strong quest for the information coupled with lobbying of government officials to try and blockade legislation. A relativist firm in this example would base decisions on industry practices and possibly take the lead and try and establish a self-regulation norm for pharmaceutical firms. In this example the information will undoubtedly impact profits and the size of the firm may also play a role in influencing which strategy to pursue. A firm concerned with justice would seek to market only to those customers for whom there is a clear-cut benefit, in the form of better treatment results and/or lower costs.

A closer look at the ethical frame of a firm involved in our third scenario, the record company seeking purchase history, reveals a few interesting options. The utilitarian stance here would emphasize potential customer satisfaction due to more focused marketing and an easier path to future purchases. The egoist firm would stress the potential sales increase as a result of this program while the relativist firm would likely benchmark rivals in the industry and act accordingly. A justice-oriented firm would seek permission from customers, i.e an opt-in approach to leveraging the customer relationship. The aggressive nature of the firm and its financial situation would also be factors in the decisionmaking process.

A firm that bases its policies on relativist ethics will need to spend more time monitoring and tracking the industry norms and standards. A firm guided by egoism in ethics will develop privacy strategies purely derived from internal analysis, stressing positive cost-benefit outcomes, with little heed to customer complaints and divergent industry practices. Companies with a strong utilitarian ethical bent will likely survey customer to measure the utility of their privacy policies to themselves and to their customers in deciding on privacy strategies. Justice oriented firms will be more likely to give greater weight to customer privacy than to the firm's profit maximization interests. As privacy strategies are clarified through the interplay of ethical frames and firm specific conditions, these need to be codified and clearly conveyed throughout the organization, to all of the firm's personnel, via communication, dialog and focused training.

Differential privacy strategies for different markets

The country and region where a firm is located provides the over-arching tenor for privacy protection; thus, a European firm operating in the U.S. might consider self-regulation as the primary mode governing privacy protection because it is the prevalent norm and accepted industry practice; however, if its ethical stance dictates greater consideration for safeguarding customer privacy, it might offer higher levels of privacy protection when compared to its competitors. Thus, firms often may find themselves with divergent approaches to privacy protection, for the same data scenarios, in different countries, and there may be a compelling marketing rationale to treat all customer privacy the same way and provide the same (high) level of privacy protection to all customers in all countries. Such a strategy may be encouraged as countries seek extra-territorial application of their privacy laws; for example, the EU attempts to require all companies doing business in the EU, including U.S. multinationals, to abide by EU data privacy regulations.

The United States and Europe have taken different philosophical postures on the data privacy protection issue and the self vs. governmental monitoring debate is very alive in the global marketplace (Scheibal and Gladstone, 2000). Specifically, the European Union has taken a firmer stance in order to provide strong legal protection of individual privacy rights. As mentioned earlier, the U.S. has enacted a patchwork of privacy related legislation, yet has maintained tolerance of a self-regulation approach by digital businesses; in the meantime, firms need to assess their relative level of compliance with the stricter regime (Pincus and Johns, 1997). The recently proposed "Safe Harbor" rules are one approach to allow the co-existence of somewhat incompatible privacy protection regimes (Hancock, 2001). Under these Safe Harbor rules, the EU allows firms and industry associations to selfcertify that their data privacy policies are in keeping with EU guidelines, with the U.S. Department of Commerce being charged with monitoring compliance and enforcing sanctions.

This raises an interesting question: when two countries or regions, such as the EU and the U.S., which trade extensively with each other, have significantly divergent data privacy protection regimes, which regime will gain ascendance? In this instance, will the EU position providing higher levels of privacy protection prevail, or will the more company-friendly U.S. self-regulatory approach become dominant. The above discussion of ethical frames underlying the various scenarios suggests that divergence is likely to continue, as ethical frameworks can differ, and will be moderated by firm-specific factors, thus leading to divergent outcomes. Future researchers may elect to incorporate additional moral philosophies, such as Kantianism, into their analyses. As far as empirically testing the various relationships set forth in the model, a methodology similar to that employed by Fritzsche and Becker (1984), in which they employed decision scenarios, or vignettes, followed by diverse responses reflective of different moral views, may be appropriate.

On the cost-benefit side, the firm must first understand the costs of compliance; the next step is to reduce such costs, through effective data base design, programs for accessing and correcting such data and security provisions to prevent unauthorized access to data. The firm also needs to monitor customer awareness of and gains from personalization and customized marketing, since such gains are the reason that the firm gathers and uses detailed customer data; if customers do not perceive that they are gaining from the firm's attempts at customized marketing, they will be more wary of the firms data collection efforts and resent the firms' invasion of their privacy. Moreover, in implementing agreed upon privacy policies, firms must pay attention to audit mechanisms, nominate and give autonomy to compliance officers, periodically survey levels of compliance achieved, communicate such results to customers and other clients, and trace the relationship between high levels of compliance and benefits to the firm such as enhanced revenues, customer loyalty and higher levels of trust.

With regard to legislation, U.S. top management with a corporate culture that emphasizes profits is likely to prefer to lobby legislators, both individually and through industry groups, so that privacy policies lean towards self-regulation, and if imposed on them, take into account industry specific issues such as the type of data being gathered and how sensitive such data is for customers, as well as the costs of compliance.

If we consider how U.S. firms have approached protecting digital privacy, a broad generalization would be that most U.S. firms have followed the letter of the law when legislation has been passed to regulate protection of individual privacy. U.S. firms might be seen as being principally following a rule utilitarian or egoism principle. The difficulty is that U.S. corporate digital privacy policies have been formulated with marketing considerations in mind and consumers have been given less attention. In part, this may stem from a long-standing tradition of junk-mail based marketing and more recently, telemarketing; using digital means to invade privacy may be seen as simply a continuation of past practice, albeit through a different channel. However, consumers are sufficiently worried about loss of privacy that serious efforts are under way to regulate digital privacy. U.S. firms can continue to fight against such regulation and seek to minimally comply with such legislation when passed, as with the current approach of financial service firms in complying with the regulations requiring them to provide their consumers with privacy notices. The notices are lengthy and obscure and few consumers understand or read them. This allows firms to proclaim compliance with the law but does little to assuage consumer concerns or reduce their unease. The likely result is that consumer anxiety will continue to build to the point that external legislation will create the protection that consumers seek and that firms are unwilling to provide of their own volition.

If firms do not develop an ethical perspective that balances their self-interest with the needs of society and consumers, they are likely to face increasing amounts of regulation. If they truly seek to manage their own future through a policy of self-regulation, they must listen to and incorporate the concerns of their customers and of society and government. The reason lies in the growing pressure from consumer interest groups and governmental agencies in regulating privacy. The increasing number of industry-specific laws that have been passed in recent years are a clear sign that consumers and lawmakers are dissatisfied with corporate approaches to privacy protection. The prognosis then is for more of the same, i.e. more legislation, unless corporations wake up and adopt a strategy that balances corporate interests with customer interests.

Our framework helps firms take into account the multiplicity of factors that should inform the privacy strategy arrived at. While ethical considerations should be at the fore, the framework does provide a model to take into account the environmental context and firm-specific controllable factors, allowing the firm to develop a strategy that is both pragmatic and ethical and tailored to its specific context and situation. The policy that emerges is more likely to meet its long-term goal of enhancing customer satisfaction and maintaining customer loyalty, which is at the heart of successful strategy implementation. The many external and subjective pressures that organizations face must also be considered when facing implementation issues, and one model cannot capture the complete set of possible influences on the decision-making process. Further, individual biases and interorganizational negotiation tactics are factors that could influence the ultimate outcome.

As more firms make the move to electronic commerce the issue of privacy protection will become increasingly important - not just what data is stored on customers in corporate databases, or which sites people visit when on the Internet, but also what they watch on digital TV and where they communicate with their wireless phones that continuously transmit location information. Firms will need to pay continuous attention to privacy issues if consumer goodwill and successful marketing are to be achieved.

Acknowledgement

The authors would like to thank two anonymous reviewers for their insightful comments.

|  |
| --- |
| **[Sidebar]** |
| Journal of Business Ethics 46: 111-126, 2003. |
| (C) 2003 Kluwer Academic Publishers. Printed in the Netherlands. |

|  |
| --- |
|  |

|  |
| --- |
| **[Reference]**  **»**   [View reference page with links](http://proquest.umi.com/pqdweb?VInst=PROD&VName=PQD&VType=PQD&RQT=594&did=405822051&Fmt=3&refType=CITEDIN&b2=d&SrchMode=1&sid=12&index=0&TS=1289602490) |
| References |
| Barry, V.: 1979, Moral Issues in Business (Wadsworth, Belmont, CA). |
| Bibas, Steven A.: 1994, 'A Contractual Approach to Data Privacy', Harvard Journal of Law &Public Policy 17(2) (Spring). |
| Blanchette, Jean-Francois and Deborah G. Johnson: 2002, 'Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness', The Information Society 18, 33-45. |
| Boatright, J.: 1999, Ethics and the Conduct of Business (Prentice-Hall, Upper Saddle River, New Jersey). |
| Caudill, E. and P. Murphy: 2000, 'Consumer Online Privacy: Legal and Ethical Issues', Journal of Public Policy and Marketing 19(1), 7-19. |
| Cavanagh, G., D. Moberg and M. Velasquez: 1981, 'The Ethics of Organizational Politics', Academy of Management Review 6, 363-374. |
| Charters, D.: 2002, 'Electronic Monitoring and Privacy Issues in Business Marketing: The Ethics of the DoubleClick Experience', Journal of Business Ethics 35(4), 243-254. |
| Computer and Internet Lawyer: 2002, 'Current Developments: Microsoft Settles FTC Charges Alleging False Security and Privacy Promises', 19(10), 32. |
| Computer and Internet Lawyer: 2002, 'Current Developments: Major Online Advertiser Agrees to Privacy Standards for Online Tracking', 19(11), 32. |
| Computer and Internet Lawyer: 2002, 'Current Developments: Eli Lilly Agrees to New Safeguards for Consumer Data', 19(11), 33. |
| DeGeorge, R.: 2000, 'Business Ethics and the Challenge of the Information Age', Business Ethics Quarterly 10(1), 63-72. |
| Donaldson, T. and P. Werhane: 1996, Ethical Issues in Business: A Philosophical Approach (Prentice-Hall, Upper Saddle River, New Jersey). |
| Eisenberg, Anne: 1996, 'Privacy and Data Collection on the Net', Scientific American 274(3) (March), 120-121. |
| Epicurus: 1963, The Philosophy of Epicurus; Letters, Doctrines, and Parallel Passages from Lucretius. Translated with commentary and an introductory essay on ancient materialism by George K. Strodach (Northwestern University Press, Evanston, IL). |
| Ferrell, O. C., J. Fraedrich and L. Ferrell: 2000, Business Ethics: Ethical Decision Making and Cases, 4th ed. (Houghton Mifflin, Boston). |
| Fritzsche, D. and H. Becker: 1984, 'Linking Managerial Behavior to Ethical Philosophy - An Empirical Investigation', Academy of Management Journal 27, 166-175. |
| Fromholz, Julia M.: 2000, 'The European Union Data Privacy Directive (Annual Review of Law and Technology)', Berkeley Technology Law Journal 15(1) (Winter). |
| George, Barbara Crutchfield, Patricia Lynch and Susan J. Marsnik: 2001, 'U.S. Multinational Employers: Navigating through the "Safe Harbor" Principles to Comply with the EU Data Privacy Directive', American Business Law Journal 38(4) (Summer). |
| Ger, Guliz and Russell W. Belk: 1996, 'Cross-Cultural Differences in Materialism', Journal of Economic Psychology 17(1), 55-77. |
| Green Heather et al.: 2000, 'Its Time for Rules in Wonderland', Business Week, Mar. 20. |
| Griffith, D. and J. Palmer: 1999, 'Leveraging the Web for Corporate Success', Business Horizons (JanuaryFebruary), 3-10. |
| Hancock Bill: 2001, '"Safe Harbor" Provision Adopters Few and Far Between', Computers & Security 20(1). |
| Hemphill, Thomas A.: 2001, 'DoubleClick and Consumer Online Privacy: An E-Commerce Lesson Learned', Business and Society Review 105(3), 361-372. |
| Introna, L. and A. Pouloudi: 1999, 'Privacy in the Information Age: Stakeholders, Interests and Values', Journal of Business Ethics 22, 27-38. |
| Jones, T.: 1991, 'Ethical Decision Making by Individuals in Organizations: An Issue-Contingent Model', Academy of Management Review 16(2), 366-395. |
| Journal of Internet Law: 2002, DoubleClick Settles. Sept. 2002, 25-26. |
| Kelly, E. and H. Rowland: 2000, 'Ethical and Online Privacy Issues in Electronic Commerce', Business Horizons (May-June), 2-12. |
| Kohlberg, L.: 1984, Philosophy of Moral Development (Harper and Row, New York). |
| Lessig Lawrence: 1999, Code and other Laws of Cyberspace (Basic Books, New York). |
| Pincus Laura B. and Johns Roger: 1997, 'Private Parts: A Global Analysis of Privacy Protection Schemes and a Proposed Innovation for their Comparative Evaluation. Journal of Business Ethics 16(12-13), 1237-1260. |
| Premeaux, S. and R. Mondy: 1993, 'Linking Management Behavior to Ethical Philosophy', Journal of Business Ethics 12, 349-357. |
| Rawls, J.: 1971, A Theory of Justice (Harvard University Press, Cambridge). |
| Reidenberg, Joel R.: 2000, 'Resolving Conflicting International Data Privacy Rules in Cyberspace', Stanford Law Review (May 2000), 1315-1370. |
| Robertson, Christopher and Ravi Sarathy: 2002, 'Digital Privacy. Executive Briefing', Business Horizons (Jan.-Feb.), 2-5. |
| Sama, L. and V. Shoaf: 2002, 'Ethics on the Web: Applying Moral-decision-making to the New Media', Journal of Business Ethics 36(1-2), 97-103. |
| Samuelson, Pamela Data: 1999, 'Privacy Law: A Study of United States Data Protection', California Law Review 87(3). |
| Scheibal, W. and J. Gladstode: 2000, 'Privacy on the Net: Europe Changes the Rules', Business Horizons (May-June), 13-18. |
| Shane, S. and S. Venkataraman: 1996, 'Renegade and Rational Championing Strategies', Organization Studies 17, 751-771. |
| Tang, Paul C.: 2000, 'The HIPAAcratic Oath: Do no Harm to Patient Data', The Physician Executive, (May-June), 50-55. |
| Trevino, L.: 1986, 'Ethical Decision Making in Organizations: A Person-Situation Interactionist Model', Academy of Management Journal 11, 601-617. |

|  |
| --- |
|  |

|  |
| --- |
| **[Author Affiliation]** |
| Ravi Sarathy |
| General Management Group, |
| Northeastern University, |
| College of Business Administration, |
| Boston, MA 02115, |
| U.S.A. |
| E-mail: r.sarathy@neu.edu |
| Christopher J. Robertson |
| General Management Group, |
| Northeastern University, |
| College of Business Administration, |
| Boston, MA 02115, |
| U.S.A. |
| E-mail: c.robertson@neu.edu |

|  |
| --- |
|  |

**References**

* [Cited by (6)](http://proquest.umi.com/pqdweb?VInst=PROD&VName=PQD&VType=PQD&RQT=594&did=405822051&Fmt=3&refType=CITEDBY&b2=d&SrchMode=1&sid=12&index=0&TS=1289602490)



**Indexing (document details)**

|  |  |
| --- | --- |
| **Subjects:** | [Electronic commerce](javascript:searchSideWays(%22SUB%22,%22Electronic%20commerce%22)),  [Customer information files](javascript:searchSideWays(%22SUB%22,%22Customer%20information%20files%22)),  [Marketing](javascript:searchSideWays(%22SUB%22,%22Marketing%22)),  [Privacy](javascript:searchSideWays(%22SUB%22,%22Privacy%22)),  [Business ethics](javascript:searchSideWays(%22SUB%22,%22Business%20ethics%22)),  [Politics](javascript:searchSideWays(%22SUB%22,%22Politics%22)),  [Studies](javascript:searchSideWays(%22SUB%22,%22Studies%22)) |
| **Classification Codes** | [1210 Politics & political behavior](javascript:void(0);),  [2400 Public relations](javascript:void(0);),  [5250 Telecommunications systems & Internet communications](javascript:void(0);),  [7000 Marketing](javascript:void(0);),  [9130 Experimental/theoretical](javascript:void(0);) |
| **Author(s):** | [Ravi Sarathy](http://proquest.umi.com/pqdweb?index=0&did=405822051&SrchMode=1&sid=12&Fmt=3&VInst=PROD&VType=PQD&CSD=24141&RQT=590&VName=PQD&TS=1289602490&clientId=29440) [[http://proquest.umi.com/images/common/profile_scholar.gif](http://proquest.umi.com/pqdweb?index=0&did=405822051&SrchMode=1&sid=12&Fmt=3&VInst=PROD&VType=PQD&CSD=24141&RQT=590&VName=PQD&TS=1289602490&clientId=29440)**profile**](http://proquest.umi.com/pqdweb?index=0&did=405822051&SrchMode=1&sid=12&Fmt=3&VInst=PROD&VType=PQD&CSD=24141&RQT=590&VName=PQD&TS=1289602490&clientId=29440),  [Christopher J Robertson](http://proquest.umi.com/pqdweb?index=0&did=405822051&SrchMode=1&sid=12&Fmt=3&VInst=PROD&VType=PQD&CSD=24128&RQT=590&VName=PQD&TS=1289602490&clientId=29440) [[http://proquest.umi.com/images/common/profile_scholar.gif](http://proquest.umi.com/pqdweb?index=0&did=405822051&SrchMode=1&sid=12&Fmt=3&VInst=PROD&VType=PQD&CSD=24128&RQT=590&VName=PQD&TS=1289602490&clientId=29440)**profile**](http://proquest.umi.com/pqdweb?index=0&did=405822051&SrchMode=1&sid=12&Fmt=3&VInst=PROD&VType=PQD&CSD=24128&RQT=590&VName=PQD&TS=1289602490&clientId=29440) |
| **Author Affiliation:** | Ravi Sarathy General Management Group, Northeastern University, College of Business Administration, Boston, MA 02115, U.S.A. E-mail: r.sarathy@neu.edu Christopher J. Robertson General Management Group, Northeastern University, College of Business Administration, Boston, MA 02115, U.S.A. E-mail: c.robertson@neu.edu |
| **Document types:** | Feature |
| **Publication title:** | [Journal of Business Ethics](http://proquest.umi.com/pqdweb?RQT=318&pmid=15840&TS=1289602490&clientId=29440&VInst=PROD&VName=PQD&VType=PQD). Dordrecht: [Aug 2003](http://proquest.umi.com/pqdweb?RQT=572&VType=PQD&VName=PQD&VInst=PROD&pmid=15840&pcid=5964271&SrchMode=3). Vol. 46, Iss. 2;  pg. 111 |
| **Source type:** | Periodical |
| **ISSN:** | 01674544 |
| **ProQuest document ID:** | 405822051 |
| **Text Word Count** | 8056 |
| **Document URL:** | http://proquest.umi.com/pqdweb?did=405822051&sid=12&Fmt=3&clientId=29440&RQT=309&VName=PQD |

|  |  |  |  |
| --- | --- | --- | --- |
| [http://proquest.umi.com/images/common/printicon.gifPrint](http://proquest.umi.com/pqdweb?index=0&sid=12&srchmode=1&vinst=PROD&fmt=3&startpage=-1&clientid=29440&vname=PQD&RQT=309&did=405822051&scaling=FULL&ts=1236293702&vtype=PQD&rqt=309&TS=1289602490&clientId=29440&cc=1&TS=1289602490)  | [http://proquest.umi.com/images/common/emailicon.gif](http://proquest.umi.com/pqdweb?RQT=563&VInst=PROD&VName=PQD&VType=PQD&sid=12&Fmt=3&did=405822051&otherFmt=2|3|10) [Email](http://proquest.umi.com/pqdweb?RQT=563&VInst=PROD&VName=PQD&VType=PQD&sid=12&Fmt=3&did=405822051&otherFmt=2|3|10)  | [http://proquest.umi.com/images/common/linkicon.gif](http://proquest.umi.com/pqdweb?RQT=569&curl=http%3A%2F%2Fproquest.umi.com%2Fpqdweb%3Fdid%3D405822051%26sid%3D12%26Fmt%3D3%26clientId%3D29440%26RQT%3D309%26VName%3DPQD&TS=1289602490) [Copy link](http://proquest.umi.com/pqdweb?RQT=569&curl=http%3A%2F%2Fproquest.umi.com%2Fpqdweb%3Fdid%3D405822051%26sid%3D12%26Fmt%3D3%26clientId%3D29440%26RQT%3D309%26VName%3DPQD&TS=1289602490)  | [http://proquest.umi.com/images/common/citeicon.gif](http://proquest.umi.com/pqdweb?RQT=568&VInst=PROD&VName=PQD&VType=PQD&Fmt=3&did=405822051&TS=1289602490) [Cite this](http://proquest.umi.com/pqdweb?RQT=568&VInst=PROD&VName=PQD&VType=PQD&Fmt=3&did=405822051&TS=1289602490)  |  Mark Document | | [Publisher Information](http://proquest.umi.com/pqdweb?RQT=318&pmid=15840&Tab=3&TS=1289602490&clientId=29440&VInst=PROD&VName=PQD&VType=PQD) | |
| **^** [Back to Top](http://proquest.umi.com/pqdweb?index=0&did=405822051&SrchMode=1&sid=12&Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1236293702&clientId=29440#top) |  | http://proquest.umi.com/images/common/x.gif                http://proquest.umi.com/images/common/x.gif |  |

Bottom of Form

Copyright © 2010 ProQuest LLC. All rights reserved. [Terms and Conditions](http://www.il.proquest.com/go/termsandconditions)

[Text-only interface](http://proquest.umi.com/pqdweb?index=0&did=405822051&TS=1236293702&SrchMode=1&sid=12&Fmt=3&VInst=PROD&VType=PQD&int=1&clientId=29440&RQT=309&VName=PQD)