Information Privacy: Legal and Ethical Decision-making

John Beachboard and Kregg Aytes
Idaho State University, Pocatello, Idaho, USA

beach@isu.edu aytekreg@isu.edu

Abstract

This essay was created for use in a business oriented IT or IS class. The purpose of this manuscript is to help students understand legal and ethical dilemmas associated with the use of information and information technology, primarily within the context of information privacy. The essay provides information that illustrates why information privacy has become such an important issue for businesses, discusses some of the relevant U.S. and international laws governing business use of customer information, and proposes a decision-making process that can be used by business managers to assist in making ethical business decisions. *The essay is not a research submission nor is it intended to represent a comprehensive review of relevant literature.*

Keywords. privacy, ethics, decision-making

Introduction

Have you ever wondered why you are asked questions about your hobbies when you fill out a warranty application? Or why your grocery store offers you discounts if you allow them to scan their shopper's card when you check out? While this essay is not about privacy concerns *per se*, the privacy issues offer a good launching point for a discussion of laws and ethics in the domains of information and technology. Personal information has long resided in the data repositories of commercial, governmental, and not-for-profit entities. But often that personal information was stored in numerous paper files or uniquely structured databases making the aggregation and sharing of it difficult and expensive. You would probably not be surprised to hear that with the numerous advances in information technology that have taken place over the last several decades, aggregating and sharing of data have become much easier and far less expensive.

However, you might be surprised to learn the extent to which information about you, such as the hobby information requested on a warranty application, is available for sale. Commercial information brokers such as Choicepoint (acquired for $3.6 billion in 2008 by Reed Elsevier, the parent company of LexisNexis) and Acxiom store massive amounts of data about individuals retrieved from a wide variety of public and private information sources including: arrest records, mortgage information, credit card purchases, utility bills, and information collected with the warranty and shoppers' cards (O'Harrow Jr., 2005; Rivlin, 2006). Robert O'Harrow argues, "almost everyone you do business with collected information about you, sold it to someone else, or sifted it for their own mercantile means" (O'Harrow Jr., 2005, p. 6).

Interestingly, in the U.S., the collection, aggregation and selling of personal data are relatively unregulated, although that is starting to change due to concerns expressed by consumer advocates regarding software techniques used by commercial enterprises to surreptitiously track online behavior.[1] Meanwhile government agencies have restrictions on the use of information they collect. So for example, the Internal Revenue Service (IRS) is prohibited from sharing tax information that might be used to locate children abducted by disgruntled former spouses dissatisfied with the results of custody decisions (Kocieniewski, 2010). Perhaps even more interesting is the fact that while law enforcement agencies can be restricted in how they directly gather potentially relevant information during criminal investigations, they do purchase such information from information brokers.[2]

It is not difficult to discern businesses' motivations for buying and selling information. Selling information can obviously be profitable, witness the purchase of Choicepoint referenced above. The business model of information brokers is to sell business-relevant information. The value of information brokers resides in their being able to combine and organize the information from multiple sources into a form that can be easily used by the purchasers. At its simplest the motivation of the information purchasers is clear as well: they want to predict consumer behaviors. They want to discern consumer attitudes that can inform the development of more desirable products, determine media consumption behavior (of consumer segments) so that product advertising can be efficiently and effectively targeted, and predict which consumers are most likely to default in paying their bills. In short, businesses are constantly seeking information to improve their business decision-making. However, there may be negative consequences of engaging in such behavior as more consumers feel their privacy is being invaded. Thus, we use the issue of privacy to launch our discussion of legal and ethical decisions arising from within the information and technology domains.

As we shall see, governments have passed numerous laws intended to protect individual rights of privacy. **Laws** are rules or regulations mandating or prohibiting certain behaviors. What makes a rule a law is that it is enacted by a legitimate governing authority. Laws, while often reflecting ethical considerations, differ from ethical norms because governments enforce their laws and penalize violators. Our **ethical values** represent our beliefs concerning what we should or should not do and may or may not be adequately reflected in the legal codes. That is, it is possible to violate your ethical values even while complying with enacted laws. In fact, there may be a time when strict compliance with the law might violate your ethical values.

Without intending to trivialize these important subjects, we approach legal compliance and ethical business conduct as a particular category of business (and personal) decisions.

Our objectives in this essay are several; they include:

1. Increasing your awareness of laws and ethical challenges relevant to the planning and use of information and technology and the business decisions they entail
2. Informing you that international laws and regulations concerning the use of information and technology can vary from those applicable in the U.S.
3. Presenting legal and ethical issues in the context of business decision-making

[1] For example, see the Wikipedia article on zombie cookies at: http://en.wikipedia.org/wiki/Zombie_cookie .

[2] For more information on privacy related issues, see the O'Harrow book referenced above and visit the Electronic Privacy Information Center's website at: http://epic.org/.

4. Introducing a simple ethical decision-making model to assist you in thinking about how to respond to ethical issues encountered in the workplace
5. Reinforcing your understanding of the potentially corrosive influence that individual cognitive biases and group influence can have on our ethical behavior

Before proceeding, we wish to clarify a problem on which this essay provides no substantive insight. If a reader happens to be disposed to committing theft or financial fraud, nothing in this essay is likely to change that disposition. If we knew how to do that, we would patent the process and become multi-millionaires. Our interest is in helping students avoid sliding down a slippery slope where aggressive business practices ultimately become illegal or unethical business behavior.

Why Legal Compliance and Ethical Conduct Constitute Business Decisions

Apart from any moral qualms one might have, legal compliance constitute business decisions because of the issue of liability. A business may be found **liable** when it or its employees engage in behaviors which incur criminal penalties (e.g., fines or jail time) or require the payment of restitution or compensation to individuals or businesses injured by those behaviors. Liability can be legally incurred even if no law has been broken. A company might be held liable for reckless behavior even if that behavior violated no specific law. For example, a company could be found guilty of reckless endangerment for failing to adequately maintain its motor vehicles.

Businesses must be concerned with minimizing direct financial liabilities resulting from illegal and unethical behavior. Beyond direct financial liabilities, businesses must also be concerned with damage to the business or brand reputation that may occur. The indirect financial damage resulting from a damaged reputation may far outweigh the direct financial penalties imposed or negotiated. So as mercenary as it may sound, there is a business calculus that can be performed to assess potential gains and losses occurring from illegal and unethical behavior. However, as indicated in the introduction, our concern is not with intentional illegal and unethical acts. In the information and technology domains, there are gray areas where businesses make decisions that have legal and ethical implications.

We lack the technology and skill to make our information systems perform with total reliability. Information assurance professionals typically offer three categories of IT service failures (McCumber 2005):

- Breach of confidentiality: when individuals are able to access and read information which they are not authorized to access
- Loss of data integrity: when data are changed or corrupted irrespective of whether it occurs as a result of human error, system mistake or malicious activity
- Disruption of service availability: when authorized users are denied access to IT services, again irrespective of whether that denial of service is the result of accidental error or an intentional service disruption.

How much investment is required to establish that the firm has acted with **due diligence**, i.e., made a "reasonable" effort to comply with applicable laws and avoid harming others? Rapidly changing technology makes the determination of what is "reasonable" complex.

Individual privacy represents one of the most heavily regulated and ethically challenging issues facing businesses today. The regulatory environment is especially complicated for global businesses which face a variety of laws and regulations depending on the countries in which they op-

erate. Due to the significance and diversity of privacy regulation and privacy's myriad ethical implications, this essay grounds its discussion of legal and ethical decision-making in the context of individual privacy.

Privacy Regulation

In the U.S., **privacy** generally refers to constitutionally guaranteed safeguards against intrusions into one's personal life and surveillance of one's personal activities, **without just cause**. U.S. privacy law differs fundamentally from the privacy laws of many other countries. A great deal of federal privacy law is designed to protect U.S. citizens from allowing governmental intrusion on personal privacy, consistent with Fourth Amendment Constitutional safeguards. For example: the **Federal Privacy Act of 1974** holds federal agencies accountable for the unauthorized release and use of personal and business information; the **Electronic Communications Act of 1986** includes numerous provisions regulating the interception of electronic communication (notably this act prohibits employer monitoring of workplace communications without prior consent); and the **Computer Matching and Privacy Act of 1988** builds on the **Privacy Act** requiring agencies to establish specific procedures to share information with each other (this is the law that the prohibits the IRS from using tax return information to help locate abducted children). The **Patriot Act of 2001**, passed in response to the 9/11 terrorist attacks on the World Trade Center and the Pentagon, is viewed by many to inappropriately weaken privacy safeguards.

However, the increasing computerization of personal information has led to regulation of the private sector in the U.S. even though those protections do not rise to the level of safeguards provided by many other countries. The **Right of Financial Privacy Act of 1978** establishes controls over depositors' bank account records. The **Electronic Funds Transfer Act of 1979** establishes safeguards for digital fund transfers. The **Financial Services Modernization (Gramm-Leach-Bliley) Act of 1999** provides limited privacy protections concerning the use of personal financial information. For example, the law requires all financial institutions to disclose their privacy policies relating to the sharing of non-public financial information and requires financial firms to create a security policy describing how the company intends to safeguard its customers' financial information. The **Health Insurance Portability and Accountability Act of 1996 (HIPAA)** was written to encourage greater use of information technology in the healthcare industry. However, recognizing concerns regarding the privacy of medical information, HIPAA directed the creation of security standards and practices to protect electronically stored and transferred healthcare information. Notable also is California's **Security Breach Notification Act of 2003** that requires firms to inform individuals if evidence suggests that their personal information has been compromised. Since California passed its laws, numerous states have passed similar notification laws increasing the cost and negative consequences of security breaches.

In the countries comprising the European Union (EU), personal privacy is considered an individual right which requires governmental protection. EU members have harmonized stringent privacy safeguards. Of particular interest to U.S. firms doing business in Europe is the prohibition against transferring personal, employee as well as customer, data to any country that lacks the security safeguards mandated by EU regulation. The U.S. and EU have negotiated **safe harbor** provisions which allow U.S. firms to comply with EU standards so that European data can be transferred to the U.S. A significant difference in the safeguards concerns the use of "opt-in" rather than "opt-out" provisions concerning control of personal information.

An "opt-in" approach, as generally required in Europe, requires consumers to explicitly give permission for personal data to be collected and used for business purposes beyond the immediate transaction (including the sharing of that data with other businesses). An "opt-out" approach, as generally used in the U.S., does not require explicit consumer permission for data to be collected and used. Instead, the "opt-out" approach requires the consumer to specifically deny the collec-

tion and use of the data by taking some specific action. As consumers are less likely to go through the effort to specifically deny permission, businesses generally obtain much more useful information in an "opt-out" situation. This information comes at some loss of privacy to the individual consumer, as he or she may not realize what information has been collected.

This section provides just a sampling of laws governing the use of information and technology by private companies and is primarily concerned with laws that require maintaining the confidentiality of specific classes of personal data. The sharing and aggregation of personal information by businesses remain largely unregulated in the U.S., permitting the information brokering firms to flourish. Maintaining data integrity of these data also poses significant concerns. The **Fair Credit Reporting Act of 1970** (as amended numerous times) establishes civil penalties for firms that are negligent in maintaining credit information. Despite the legislation described above, consumer advocates have argued that companies routinely violate provisions of relevant federal and state privacy laws (see for example EPIC letter to Federal Trade Commission concerning information broker violations of Federal Credit Reporting Act at: http://epic.org/privacy/choicepoint/fcraltr12.16.04.html.

These laws establish requirements for the creation of technical and operational standards with which businesses are obligated to comply. We need to recognize that the standards established by these laws are not and probably cannot be absolutely clear. Businesses must make investment and operational decisions that determine the quality of legal compliance achieved.

The Ethics of Privacy

We identified some of the practices of major information brokers in the introductory section. In this section we focus more specifically on the actions of online retailers, information brokers and advertising/marketing agencies to identify practices that, while not necessarily illegal, raise ethical concerns with respect to personal privacy.

Most online commercial sites set **cookies**, small text files placed by web servers on the (web) browsers accessing the website. Cookies provide a means for maintaining the browsing session. For example, if you are entering a purchase in the shopping cart on Amazon.com, it sets a cookie that allows you to continue shopping and then return to the cart without losing the order that you had already started. However, the web server is able to place additional information cookies that can be used to track your searches and the pages you actually visited on the website, i.e., your **clickstream**. If you have never visited the site before and have not filled out any forms on the website, the webserver only learns your IP address and the type of browser that you are using. However, if you have filled out a form or made a purchase from that site and are using the same computer, the web server may be able to associate your clickstream with information that can personally identify you. Whether the server does or does not do this depends on the business practices and voluntary privacy policies that the web vendor chooses to employ.

Below is an example of the type of information that can be collected by a commercial site. The following excerpts were drawn from Amazon.com's privacy notice (last updated October 1, 2008).

Information You Give Us [Amazon.com]

You provide most such information when you search, buy, bid, post, participate in a contest or questionnaire, or communicate with customer service. For example, you provide information when you search for a product; place an order through Amazon.com or one of our third-party sellers; provide information in Your Account (and you might have more than one if you have used more than one e-mail address when shopping with us) or Your Profile; communicate with us by phone, e-mail, or otherwise; complete a questionnaire or a contest entry form; compile Wish Lists or other gift registries; provide employer information when opening a corporate account; participate in Discussion Boards or other community features; provide and rate Reviews; specify a Special Occasion Reminder; share information with Amazon Friends; and employ other Personal Notification Services, such as Available to Order Notifications. As a result of those actions, you might supply us with such information as your name, address, and phone numbers; credit card information; people to whom purchases have been shipped, including addresses and phone number; people (with addresses and phone numbers) listed in 1-Click settings; e-mail addresses of Amazon Friends and other people; content of reviews and e-mails to us; personal description and photograph in Your Profile; and financial information, including Social Security and driver's license numbers.

But other information can also be gathered by Amazon.com affiliates while you are visiting Amazon's website.

Amazon makes extensive use of data it collects to market its products as well as the products of affiliated businesses. Although not legally constrained from doing so, Amazon states that it has decided not to sell information it collects.[3] With approximately 100 million registered accounts, an immense variety of products sold, and the number of product searches conducted on its website, Amazon is sitting on a goldmine of marketing data. Having already collected the data, why might Amazon choose not to establish a new revenue stream by selling these data? While we do not have "insider" information regarding how Amazon made the "business decision" not to sell customer data, we can identify a number of possible rationales.

Third-Party Advertisers and Links to Other Websites

Our site includes third-party advertising and links to other Web sites. We do not provide any personally identifiable customer information to these advertisers or third-party Web sites. Click here for more information about our Advertising Policies and Specifications.

These third-party Web sites and advertisers, or Internet advertising companies working on their behalf, sometimes use technology to send (or "serve") the advertisements that appear on our Web site directly to your browser. They automatically receive your IP address when this happens. They may also use cookies, JavaScript, web beacons (also known as action tags or single-pixel gifs), and other technologies to measure the effectiveness of their ads and to personalize advertising content. *We do not have access to or control over cookies or other features that they may use, and the information practices of these advertisers and third-party Web sites are not covered by this Privacy Notice.* [Emphasis added]

The decision not to market and sell customer data could be based purely on a financial calculation. Book and DVD searching and sales data are fairly revealing indicators of consumer interests. The decision not to sell customer data might be due to a concern that purchase of Amazon customer data by potential Amazon competitors might work to Amazon's detriment. If competitors proved more effective in mining the data and creating more effective marketing strategies, Amazon might suffer a net loss in sales due to increased competition. Amazon also might have

[3] Amazon is not able to guarantee the practices of third-party websites and advertisers placing ads on Amazon's website.

concluded that customers unhappy about having their information marketed might stop shopping at Amazon, thus resulting in lost sales.

But the business decision might be driven by ethical considerations as well. The majority of consumers do not pay much attention to privacy policies and many do not expend too much energy worrying about what might be done with their purchasing and searching information. Despite the evidence of consumer apathy regarding privacy protections, Amazon might simply have concluded that not selling the data was simply the "right" thing to do. More than likely, all of these considerations (and probably some not identified) influenced Amazon's business decision.[4]

A Process for Making Ethical Business Decisions

Much has been written on ethical decision-making. The only conclusion that is universally agreed upon in the literature is that there is no "workable list of 'do this' or 'don't do that.'" Business professionals will continue to make tough ethical decisions.[5] However, we do think it useful to look at how a typical five-step decision-making model might be adapted for the purposes of ethical decision-making.

At its most basic level, that decision-making model presented consisted of these steps:

1. Forming the decision-making team (or participants)
2. Identifying the problem driving the decision-making process
3. Generating alternative courses of action
4. Formulating and applying the decision model and measures
5. Implementing and evaluating the results of the decision

These steps can be slightly reformulated to suggest a simple and potentially useful framework for making ethical business decisions (see Figure 1). This five-step ethical decision-making framework is described below.

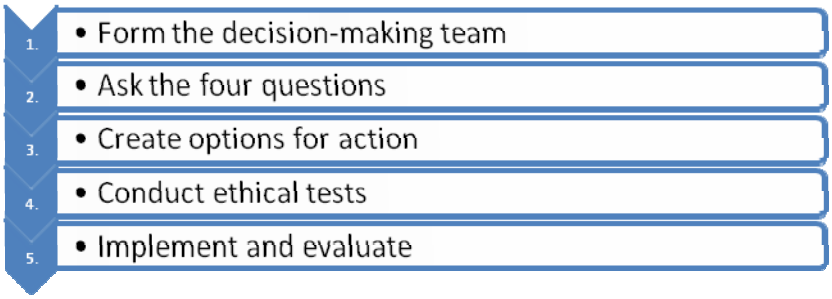

Figure 1 Four step ethical decision-making framework

Step 1. Form the Decision-Making Team

We typically think of ethical decision-making in individual terms. But in business we also need to consider the organizational consequences of ethical decisions. So, just as with organizational decisions concerning the selection of organizational strategy, businesses should consider who should participate in making ethical decisions. With respect to regulatory compliance and techni-

[4] Brief articles describing related issues Facebook and Microsoft have wrestled with are available at: http://www.techflash.com/seattle/2010/08/wsj_report_details_microsofts_internal_wrangling_over_ie_privacy.html and http://online.wsj.com/article/SB10001424052748704912004575252723109845974.html.

[5] This section adopts and adapts an ethical decision-making model developed by Kathy Lund-Dean and presented in Katz and Green's small business textbook (2007, p. 34).

cal decisions impacting customer privacy, business owners and corporate boards of directors should be involved as they will bear ultimate responsibility for the business consequences emanating from such decisions. Of course, these key decision-makers may find it useful to consult with consumers and other concerned stakeholders. However, business professionals must recognize that the inclusion of appropriate participants in making ethical decisions for a business does not absolve individuals from the consequences of their personal ethical choices.

Step 2. Defining the Ethical Problem: Four Questions

How do you know if you are facing an ethical decision? A good way to tell is by considering what you propose to do and then answering the following four questions (Hosmer, 1994):

1. Who will be hurt, and how badly?
2. Who will benefit, and how much?
3. What do you owe others, if anything?
4. What do others owe you, if anything?

We believe that honest and sincere answers to these four questions define the ethical dilemma facing the business. Yet it is quite likely that you may not be able to answer any of these questions with complete accuracy. That limitation really underscores the admonition to be honest and sincere. Ethical issues seem to evaporate once we convince ourselves that no one will be badly hurt and that our obligations are non-existent even if "unfortunate consequences" might occur.

Step 3. Create Options for Action

Poor ethical decisions are sometimes made because businesses or individuals did not really perceive that choices were available. Choices are always available. In the worst cases, none of them happens to be very appealing. First you want to check for the obvious solution, i.e., simply not to engage in the behavior you think creates the ethical dilemma. But if you determine that the behavior is required, there might be obvious solutions that would mitigate the harm.

We can use the click-tracking capability discussed above as an example of a potential ethical dilemma. Amazon.com has the ability to collect very detailed information about their customers and to a large extent can attribute that behavior to a specific individual. That information has a monetary value both for Amazon and for other commercial entities. Amazon could choose not to collect the information, making the problem non-existent. Or it can adopt a variety of policies regulating how the information collected can be used. If these policies are adequately communicated, customers can choose whether or not they want to shop at Amazon.com. However, if Amazon understands that most customers will not take the time to read its privacy policies, does it still have an ethical obligation to more effectively communicate its privacy policies to its customers?

Businesses may also consider creative alternatives. For example, if Amazon decided to sell its data, it could anonymize it first (albeit lowering its commercial value) or reward customer agreement by providing some type of benefit (e.g., the discounts offered to shoppers willing to scan their shopper cards). The important point is not to think that businesses are limited to a binary set of alternatives.

Next it is important to make sure that the firm truly understands the implications of each option; it needs to fill in the details. In the above example, Amazon would want to ensure that it fully understands its legal obligations relative to the choices under consideration. As discussed above, the legal requirements may vary from country to country, so filling in the details might be a non-trivial task. Sometimes decision-makers focus so strongly on the intended consequences of their actions that they fail to consider unintended consequences which could have been anticipated

given some thought. Such analyses might reveal that the costs of an option are too high or the negative consequences are too severe; then the firm might want to develop new alternatives.

Step 4. Apply Ethical Tests

Researchers in business ethics have studied ancient and modern philosophies and religious codes to develop moral philosophies and principles that can be used to guide ethical decision-making. Ironically, universal consensus has not been reached. We briefly touch upon ethical tests most commonly identified in the business ethics literature.

We start with the question of whether the proposed action is legal. Strictly speaking, we should maintain a firm distinction between legal questions and ethical questions. Laws do not address all moral dilemmas so there can be times when behavior judged to be legal is nonetheless considered unethical. We raise the issue here because we need to acknowledge that the business environment is a tough and competitive environment. Think about how often you have heard sports and military metaphors used in discussing business strategies and practices. Tough-minded business persons might conclude that if it's legal, they can ignore the ethical issues. We do not endorse such a view, but we recognize that such views exist.

Assuming that the firm wishes to operate under a higher set of ethical standards, there are four ethical tests commonly described in the literature. These include:

1. **Utilitarianism**. Is my solution the best thing for the largest number of people? The idea of selecting a course of action based on achieving the greatest good for the greatest number is appealing, but it turns out that it is fairly hard to apply. The trick lies in identifying all the possibly relevant stakeholders and making reasonably accurate "what's best" calculations.
2. **Universalism.** What if everyone does what I want to do? What kind of world would it be? The idea originates with German philosopher Immanuel Kant. While Kant was a religious man, he sought to create an ethics that could be grounded in human reason. He identified moral imperatives that should not be violated irrespective of the consequences.
3. **Golden rule.** Am I treating others as I would wish to be treated? This is an ethical test represented in many religious traditions. The golden rule is appealing in that it provides some criteria for judgment to temper utilitarian and universal ethical principles. But with the heavier reliance on human judgment, we must consider more strongly the issues of personal honesty and our capacity for self-deception. Is this really how you would wish to be treated, or have you simply convinced yourself?
4. **Billboard Principle.** What if my decision were advertised on a billboard? Probably less an ethical principle than a useful rule-of-thumb for businesses, the billboard principle asks whether you would be proud or somewhat ashamed were your decision to be widely publicized.

When making a tough, ethical decision, we advocate that you examine the decision or the ethical dilemma using all four tests. You can then ask yourself which criteria seem most likely to influence your thinking on the issue. Do the consequences appear to matter more, or do the principles seem more important to your thinking than the anticipated consequences? If you find yourself following your principles in one situation while leaning toward weighing the consequences more heavily in another, do not be surprised. Behavioral scientists studying ethical decision-making have found that situations and context do matter to the human decision-maker (Hauser 2006). For example, a business may make a commitment to protect the privacy of its customers' online practices. However, if a business manager were convinced that breaching a customer's privacy might result in saving an innocent's person's life, the manager might judge the consequences sufficient

to warrant breaching a contractual promise to a customer. Unlike philosophers, we tend to be a bit more flexible when choosing which principles are relevant to the specific decision.

Step 5. Implement and Evaluate Your Decision

Of course, we all realize that it is one thing to decide to do something and it is another to actually execute that decision. Too often we have seen examples reported in the newspaper where corporate practices did not reflect espoused corporate ideals. We need to monitor how ethical decisions are actually implemented. Furthermore, business managers should take the time to evaluate the consequence of their ethical decisions. Are you satisfied with the consequences? Have you or your team adequately understand the ethical dilemma? Did you or your team apply appropriate ethical tests? In short, are you sufficiently satisfied with the results of your decisions that you would repeat them should similar circumstances arise? If not, you want to understand why not and think about what you should do differently the next time.

Take-aways

We have used the issue of privacy to introduce you to the idea that some decisions regarding the use of information and technology have legal and ethical consequences. Of course, privacy is not the only IT issue that has legal consequences. Other examples of issues are: management of intellectual property, legal and ethical liabilities resulting from system failures, cyber-crime, and misuse of corporate resources. However, we think the issue of privacy is especially suited to our needs because:

- There are laws and regulations that specifically address privacy.
- These laws are not necessarily consistent from state to state (within the United States) and global businesses need to recognize that at least some other countries (e.g., Australia, Canada and members of the European Union) take significantly different legal approaches to protecting consumer privacy.
- And finally, beyond the safeguards to consumers and employees provided by law, there are a host of ethical issues that should be considered in determining how valuable information resources are managed and used.

In closing, we suggest that readers consider the cognitive biases and dysfunctional group behaviors reported in the business decision-making literature (Kahneman et al., 2011). Cognitive biases and groupthink behaviors are typically addressed in the context of straightforward business decisions. Yet ethical dilemmas can seriously challenge our desire to minimize uncertainty and maintain positive self- and group-images. Thus it is especially important to consider the possibility that we may unconsciously filter out information that disconfirms what we wish were true and distort the decision-making process described above. If you fear that these pre-dispositions are strongly in play, it may be useful to request an outside party, having no financial stake in the decision, to review the decision-making process.

References

Hauser, M. (2006). *Moral minds: How nature designed our universal sense of right and wrong*. New York, NY: Ecco.

Hosmer, L. T. (1994). *Moral leadership in business*. New York, NY: McGraw-Hill Irwin.

Kahneman, D., Lovallo, D., & Sibony, O. (2011). Before you make that big decision... *Harvard Business Review, 89*(6), 50-50.

Katz, J. A., & Green, R. P. (2007). *Entrepreneurial small business*. Boston, MA: McGraw-Hill Irwin.

Kocieniewski, D. (2010). I.R.S. sits on data point to missing children. *New York Times, Business Day*. Retrieved 24 November 2010, from http://www.nytimes.com/2010/11/13/business/13missing.html

McCumber, J. (2005). *Assessing and Managing Security Risk in IT Systems: A Structured Methodology*. Boca Raton, FL: Auerbach Publications.

O'Harrow Jr., R. (2005). *No place to hide*. New York, NY: Free Press.

Rivlin, G. (2006, 12/November). Keeping your enemies close. *New York Times, Business Day*. Retrieved 24 November 2010, from http://www.nytimes.com/2006/11/12/business/yourmoney/12choice.html?pagewanted=1&_r=1

Biographies

John C. Beachboard joined the Computer Information Systems faculty at Idaho State University in 2001. He completed the Ph.D. in Information Transfer and the M.S. in Information Resources Management at the School of Information Studies, Syracuse University. He holds an M.S. in Business Administration from Boston University and a B.S. in Public Administration from the University of Arizona. Dr. Beachboard has taught graduate courses in research methods, project management, and IT use in business, and undergraduate courses in IT management and systems architectures. He has held staff and management positions developing, implementing and operating information and telecommunications systems for the Department of Defense. He is keenly interested in the development, application and effectiveness of information technology management policies in the private and public sectors.

Kregg Aytes has been a member of the Computer Information Systems faculty at Idaho State University since 1993. He completed his Ph.D. at the University of Arizona in that same year. Kregg teaches graduate and undergraduate courses in CIS, served as CIS Department Chair, and has been Associate Dean since 2008. His research interests include information security, collaborative technologies and social media use by entrepreneurs. He also has a strong love of teaching and is interested in the application of IS content and skills across the business school curriculum.