Journal of Enterprise Information Management

Data mining: an ethical baseline for online privacy policies

Matthew D Dean Dinah M Payne Brett J.L. Landry

Data mining: an ethical baseline for online privacy policies

Matthew D. Dean
School of Business, University of Southern Maine, Portland, Maine, USA
Dinah M. Payne
College of Business Administration, University of New Orleans, New Orleans, Louisiana, USA, and
Brett J.L. Landry
College of Business, University of Dallas, Irving, Texas, USA

Received 18 April 2014
Revised 20 June 2014
30 September 2014
26 March 2015
5 August 2015
12 September 2015
Accepted 18 September 2015

Abstract

Purpose – The purpose of this paper is to advocate for and provide guidance for the development of a code of ethical conduct surrounding online privacy policies, including those concerning data mining. The hope is that this research generates thoughtful discussion on the issue of how to make data mining more effective for the business stakeholder while at the same time making it a process done in an ethical way that remains effective for the consumer. The recognition of the privacy rights of data mining subjects is paramount within this discussion.

Design/methodology/approach – The authors derive foundational principles for ethical data mining. First, philosophical literature on moral principles is used as the theoretical foundation. Then, using existing frameworks, including legislation and regulations from a range of jurisdictions, a compilation of foundational principles was derived. This compilation was then evaluated and honed through the integration of stakeholder perspective and the assimilation of moral and philosophical precepts. Evaluating a sample of privacy policies hints that current practice does not meet the proposed principles, indicating a need for changes in the way data mining is performed.

Findings – A comprehensive framework for the development a contemporary code of conduct and proposed ethical practices for online data mining was constructed.

Research limitations/implications – This paper provides a configuration upon which a code of ethical conduct for performing data mining, tailored to meet the particular needs of any organization, can be designed.

Practical implications – The implications of data mining, and a code of ethical conduct regulating it, are far-reaching. Implementation of such principles serve to improve consumer and stakeholder confidence, ensure the enduring compliance of data providers and the integrity of its collectors, and foster confidence in the security of data mining.

Originality/value – Existing legal mandates alone are insufficient to properly regulate data mining, therefore supplemental reference to ethical considerations and stakeholder interest is required. The adoption of a functional code of general application is essential to address the increasing proliferation of apprehension regarding online privacy.

Keywords Data mining, Ethics, Data subjects, Online privacy

Paper type Conceptual paper

Introduction: motivation and research question

With the proliferation of online services comes the explosion of data that is generated by consumers and collected by the businesses that offer these services. Subsequently, many of these businesses are using analytics, such as data mining, to help them understand their customers better. This understanding, in turn, can benefit the consumer if the provider is able to discern and predict patterns in the consumer's future use. While many consumers of these online services are aware (at least to some extent) that the business may be mining their data, what if a consumer does not want his

Journal of Enterprise Information Management
Vol. 29 No. 4, 2016
pp. 482-504
© Emerald Group Publishing Limited
1741-0398
DOI 10.1108/JEIM-04-2014-0040

private information discovered and/or used by anyone? In circumstances where confidentiality is desired, the practical, moral, and technical challenges to maintaining privacy are immense. The practice of data mining presents an abundance of issues, and a correspondingly wide array of perspectives on its proper handling.

Pearson (2009) reports that there is concern among consumers that companies put their data to uses of which the consumer is unaware. In addition, there is pervasive trepidation that commercially sensitive information is not secure. A study performed by Tsai *et al.* (2011) revealed that 70 percent of the respondents did not believe that privacy policies are easily understood. Indeed, often the policies go unread, and the majority of consumers do not fully comprehend the significance of privacy seals.

Finally, from a very broad perspective, the Big Brother syndrome frightens people (Cook and Cook, 2003; DeGeorge, 2010). DeGeorge (2010) describes the concept as:

> […] the fear of many people concerning computers and privacy […] Big Brother, the government or someone else – can at least in theory assemble all the information about us and use it for a variety of purposes. There may be errors that we do not know about, that we have no way to correct, and that yet are used to make decisions about us. Some people fear that their privacy is invaded in the process. The capacity for collecting, storing, and retrieving information far exceeds anything generations prior to ours had to face (p. 467).

As much as consumers fear the potential loss of privacy and associated difficulties (i.e. improper reporting of information or sharing, retention of incorrect information, etc.), they also often want to benefit from the use of data mining (i.e. the better targeting of marketing, the patterns of information discovered that could benefit us, etc.).

The ultimate aim of this paper is the advocacy of a code of ethical conduct to be used in the formulation of online privacy policies, as well as to provide a list of proposed practices businesses could adopt to mitigate consumer concern about online privacy. The paper sets out to accomplish this by answering three research questions:

RQ1. If there are common principles that may be identified to form the basis of online privacy policies?

RQ2. If there are well-established ethical frameworks upon which firms could base their online privacy policies?

RQ3. What are some proposed practices for the development of and adherence to effective online privacy policies?

To ensure the efficacy of a dialogue about the ethics of online privacy policies, this paper first sets forth some initial definitions associated with the concepts that form the foundation of these policies. The next section addresses the benefits and costs associated with data mining, as well as some of its many uses. Stakeholders' perspectives are then addressed. A comprehensive code of ethics will require that all stakeholders' concerns are noted and managed. Subsequently, we examine the ethics of data mining through reference to moral precept. We then review a number of globally existing frameworks found in legislation and regulations. It is from that review that we derive the principles we want to include in our comprehensive code of ethics for data mining. Finally this code of ethics is compared against a sample of actual online privacy policy statements to help determine where gaps exist between our proposed practices and current practice. It is noteworthy that we do not present this paper as an empirical one in a traditional sense, incorporating statistical analyses of surveys done. Rather, this paper is based on the authors' identification of general codes of conduct for online privacy and the in-depth review of those provisions compared against long established and more broadly known ethical principles. It is in fact this qualitative analysis that lends originality to this work: ethics can be subjective by its very nature and our analysis is an attempt to provide some structure to what might be considered too subjective a field for the provision of morally justifiable decisions regarding online privacy issues.

Research background

Data mining

Van Wel and Royakkers (2004) define data mining as the "process of extracting previously unknown information from (usually large quantities) of data, which can, in the right context, lead to knowledge" (p. 129). They further note that data mining is really just one step in the knowledge and discovery process. Into the mix, they also add the idea that web-data mining or web-mining is "the whole of data mining and related techniques that are used to automatically discover and extract information from web documents and services" (p. 129). This is by far the broadest definition of the concept, and the one used in this paper. It is the broadest kind of data mining that needs the safeguards of an ethical code of conduct to prevent invasion of privacy or other related harm to society. Data protection is the broadest appellation for what we intend: our hope is that the guiding principles we develop, along with our proposed practices, will provide a solid starting point for businesses as they improve their data protection policies. As will be evidenced in our proposed practices, the protection of data is of paramount importance.

Privacy and the right to privacy

The International Security, Trust, and Privacy Alliance (ISTPA) (2001) Framework Project reports that US Supreme Court Justice Louis Brandeis defined privacy as a negative right – the right to be let alone. Another definition provided by the report classifies privacy as the right to control information about oneself even after having communicated it to others. Pearson (2009) describes privacy as a fundamental human right, "enshrined in the United Nations Universal Declaration of Human Rights and the European Convention on Human Rights" (p. 1). Fule and Roddick (2004) identify privacy as an individual's desire and ability to keep certain information about himself secret. Jain *et al.* (2011) suggest that the mere word "mining" in "data mining" comports with the concept that individuals wish to maintain some level of privacy for some personal information.

The ISTPA (2001) Framework Project suggests that, consistent with the right to privacy, individuals have the right to decide how information about them is shared, by whom and with whom it is shared, and to what extent. In their presentation, the International Security, Trust, and Privacy Alliance Framework Project also found it important to define the concepts of security and trust. Security is the creation and maintenance of protections of personal information. Trust is garnered from consumers when assurances that personal information will be processed in a sustainably secure way accompanies the delivery of value. DeGeorge (2010) suggests that no one has the right to know personal facts and information of another unless necessary to prevent harm to others. For example, he asserts that surreptitious surveillance or wiretapping are violations of privacy not merited except in certain limited circumstances. If even the definitions of the basic concepts associated with privacy are so complicated, clearly the achievement of an effective, reasonable online privacy policy is fraught with difficulty. It is because of this reason that we develop our principles and propose practices that we believe will aid companies as they develop and grow their online privacy policy.

Benefits, costs, and uses of data mining

The reasons for using data mining are numerous. The variety of benefits gained from data mining span industries and is now generally understood. Jackson (2002) enumerates many of these benefits. As Thibodeau (2002) notes, with opt-in systems, "residents may be excluded from the kind of promotional offers and information that data sharing allows" (p. 1). Monash (2006) "united" data mining uses in business using the moniker of customer-offer targeting. He cites national security, antifraud efforts, and crime prevention as legitimate uses of data mining, along with the tracking of defective products. Finally, Monash stresses the importance of data mining in the areas of health care and research. Cook and Cook (2003) base their uses of data mining firmly in the realm of business: "customers expect business to not only meet their needs but also anticipate them" (p. 395).

In addition to the benefits associated with data mining, there are a variety of costs. These costs are sufficiently weighty as to cause concern over the practice of data mining. Fule and Roddick (2004) have suggested that there is increased apprehension over the abuse of sensitive information. Van Wel and Royakkers (2004) find that loss of individualism is a prevalent cause of consumer anxiety. The use of pattern detection to determine consumer trends dulls the sharpness of individual identity, thereby making "cattle" out of everyone. Interestingly, this unease results from the very purpose for data mining – to build knowledge of trends to better serve the individual consumer by tailoring business offerings. Ware (2007) and Cranor (2005) both identify other problems as being the lack of uniformity with respect to the legal treatment of data mining in various jurisdictions. By its very nature, the internet is an interstate and international phenomenon making it difficult and complex to uniformly regulate. Cook and Cook (2003) provide a comprehensive listing of the benefits and costs of data mining, and divide the benefits and costs into categories related to business, individuals, and society and is a good source of information.

Hoffman (2012), Jackson (2002), Monash (2006), and Orentlicher (2010) all identify industries or organizations that utilize data mining. Hoffman and Monash detail government uses of data mining, as well as others including, but not limited to, medical and defect research. Orentlicher presents an interesting picture of the medical field as populated by pharmaceutical companies which track prescriptions written by doctors, who are then pressured to prescribe certain drugs. The compulsion to do so emanates from the pharmaceutical representative who knows the doctor's prescribing history and urges more prescriptions of the drug he is selling, whether that is in the patient's best interests or not. In a comprehensive study of corporate privacy policies, the Ponemon Institute (2006) identified nine industries that benefit from data mining: financial services, consumer products, manufacturing, the pharmaceutical industry, technology/services, retail, telecommunications, energy, and transportation. Jackson (2002) also provides a large list of industries that benefit from data mining.

The perspectives: stakeholders and issues

"A stakeholder is any individual, group, organization or institution that can affect, as well as be affected by, an individual's, group's, organization's or institution's policy or policies" (Wood-Harper *et al.*, 1996, p. 71). Stakeholders can be a wide array of people or entities. Any person that can be positively or negatively affected by some behavior is a stakeholder of those engaging in that behavior. In a study reviewing Information Technology (IT) professionals, Payne and Landry (2005) include both computing professionals and the end-user of the goods/services as stakeholders. Earp *et al.* (2002) also include in their list of stakeholders IT practitioners, policy makers and consumers. Jackson (2002) lists "actors" in data mining. These stakeholders include project leaders, data mining clients, data mining analysts, data mining engineers, and IT analysts. She further identifies servers and proxy-servers. Government agencies that have some oversight of, and interest in, the collection of personal information include the Department of Homeland Security, the Federal Trade Commission, the Department of Defense, and the Transportation Security Administration are also potential stakeholders (Baumer *et al.*, 2004). Figure 1 is a representation of all stakeholders listed above.

One stakeholder meriting special attention is the IT professional who has been asked to collect information on data subjects. This individual faces massive pressure from his employers to find salient information trends, often so that management can increase sales. He is also subject to two other forms of anxiety. First, his own sense of morality is involved. Most individuals are unable to ease their ethical concerns by relying on the "I was told to do something, so I did" approach. Professionals are even less likely to be satisfied by this rationalization (DeGeorge, 2010). Second, the pressure is mounting to have more legal and societal constraints placed on data mining. Therefore, not only does the IT professional have to grapple with his own sense of what is right, but he is also subject to increasing legal and business regulation. Cook and Cook (2003) note that IT professionals will face increasing numbers of ethical dilemmas with regard to data mining and privacy issues. As early as 1965, leaders in the field of computer technology acknowledged the fact that "[computer professionals] will have thrust upon us much of the responsibility of preserving this right [to privacy]" (Ware, 2007, p. 1).

Upon review of all the stakeholders and parties involved in data mining, there are a number of labels that can be used. The suppliers of data can be labeled as consumers, end-users, or any of the other stakeholders listed here. The IT professional described above conducting data mining is also a user, so that label is unclear. Additionally, other businesses could be consumers of data as third party data mining efforts as well as being the data supplier. To eliminate this confusion, the suppliers of data whether the consumers are individuals, businesses, or government, will be referred to as data subjects. The businesses that collect the data as well as the professionals that conduct data mining will be referred to as data miners.

Now that the stakeholders have been identified, we turn to the larger issues associated with privacy policies. Perspectives are presented that represent the position

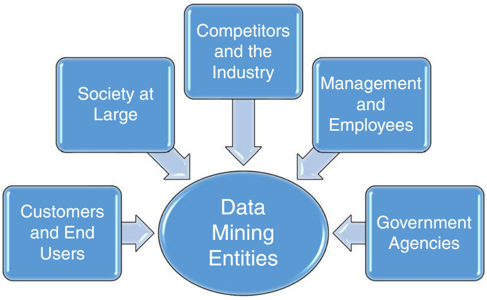

Figure 1.
Stakeholders in the data mining privacy debate

of various groups of people on issues germane to data mining. Payne and Trumbach (2009), Culnan and Bies (2003), and Earp *et al.* (2002) all identify different perspectives from which to view data mining privacy issues. These can be summarized into three perspectives – those relating to the consumer/society, those relating to the business, and the legal perspectives. The consumer/social and business perspectives are mirror images directed at each other. These perspectives recognize that consumers/society and businesses alike have rights and responsibilities to each other to exercise care, good faith, and competence in data mining activities. The other perspective is legal in orientation. Both the letter of the law and the spirit of the law should be recognized and observed. The perspectives are set out in more detail in Table I, where each perspective has associated with it our derived principle.

While the discourse about stakeholders and perspectives is vital, another important element to this discussion is the technological aspect. Gurses *et al.* (2011) assert that technology is a source of privacy protection: engineering privacy by design. They warn, however, that before privacy by design can be feasible, the ethical, legal, and political elements should be reviewed: a mere "checklist" of the right and wrong methodologies for data mining is not an appropriate solution to the questions of online privacy. Indeed, they note that such elements constitute issues beyond the expertise of engineering: while technical solutions should be part of the solution, it cannot be the whole solution, begging the question of how to organize the ethical, legal, and political elements of the problem. Our solution is the proposal of a set of guidelines of ethical behavior based on the practical and moral frameworks provided here.

The moral issue

To examine the ethics of data mining, cultural and moral norms must first be examined. These norms form the determinants of what society believes is right or wrong, ethical or unethical. There are many definitions of culture, reflecting shades of similarities and difference. Culture has been defined as the shared implicit beliefs and tacit values that identify each culture as unique. Alas (2006) describes culture as the entire set of social norms and responses that condition people's behavior – they are acquired and inculcated, not inherited. Culture has also been defined as shared motives, values, beliefs, identities, and interpretations achieved from the common experience of the group over generations. It reflects a group's way of relating to their environment and to each other (Hofstede, 1980; Schein, 1985; Ma, 2010). Values are derived from culture and are inherently the basis of a possible code of ethics for data mining. Velasquez (1999) and Joyner *et al.* (2002) suggest that what society values are that which society deems as socially or personally desirable.

Fule and Roddick (2004) define ethics as a "set of moral principles or a system of values which guide the behavior of individuals and organizations. It is the *correct* way of doing things which as judged by society and often enforced through law. To act ethically involves acting for the benefit of the community. It is entirely possible to act unethically yet legally" (p. 1). Ethics spring from the values groups and individual members of a culture hold. Ethics has also been defined as the comprehension of right and wrong (Carroll, 1979; Freeman and Gilbert, 1988). Velasquez (1999) suggests that the study of ethics also involves one's ability to choose between right and wrong, good or bad. In the development of any code of ethics, it is noteworthy that a case of determination of right and wrong is rare. Most situations with ethical overtones are not black and white, but gray, thereby making some determinations very difficult, regardless of governmental or ethically mandated provisions (Stevens *et al.*, 2005; Watson, 2006) (Figure 2).

Table I.
Three perspectives on the issue of online privacy policies

Payne and Trumbach (2009)	Culnan and Bies (2003)	Earp *et al.* (2002)	Principle derived
Legal perspective The letter of the law, of which there are many, would be followed in the collection and usage policies of data collectors	*Activist perspective* If left unchecked, the pursuit and use of personal information will result in violations of privacy, to the detriment of society as a whole: the spirit of the law is at least equally important to the letter of the law	*Legal perspective* There are legal standards to be used in the collection and use of personal information, including the use of binding, contractual agreements between the consumer and the firm	*Legal perspective* Both the letter of the law and the spirit of the law must be observed
Consumer perspective Consumers are required to be assured of anonymity of their information There should be clear disclosure of privacy policies Voluntary participation in data collection is necessary Reasonable time constraints on the use and sharing of personal information is mandated Trust should be fostered among stakeholders in personal information exchange	*Centrist perspective* Recognition that business has a need to information to aid consumers in consumer transactions to the benefit of both groups, while consumers whose personal information is sought have a solid right to privacy	*Consumer/social perspective* The relationship between the consumer and the organization is critically important to the profitable, social conduct of business	*Consumer/social perspective* Consumers and business alike have rights and responsibilities with regard to each other to exercise care, good faith and competence
Business perspective Respect for communication to stakeholders of values to which the firm is committed regarding privacy policies is mandated The integration of these values into strategic decision-making processes is required Supports to reinforce privacy policy principles should be developed	*Corporate perspective* That business is the primary engine that creates and perpetuates economic growth for society and its inhabitants must be acknowledged This perspective espouses the pursuit and use of personal information as an efficacious tool to insure economic and personal prosperity for the firm, society, and individuals	*Business perspective* That firms have goals and practices to achieve the goals that are constrained by the legal and technical perspectives must be recognized. The technology that is used in the collection and use of the information is a useful tool	*Business perspective* Consumers and business alike have rights and responsibilities with regard to each other to exercise care, good faith and competence

Moral codes of conduct

Codes of ethics should be established for sound business reasons, not simply because of external pressure or because "everyone is doing it." Codes of ethics should be established at the highest moral level, thus providing the firm or person making reference to the code the standards of conduct for which to strive (Raiborn and Payne, 1990).

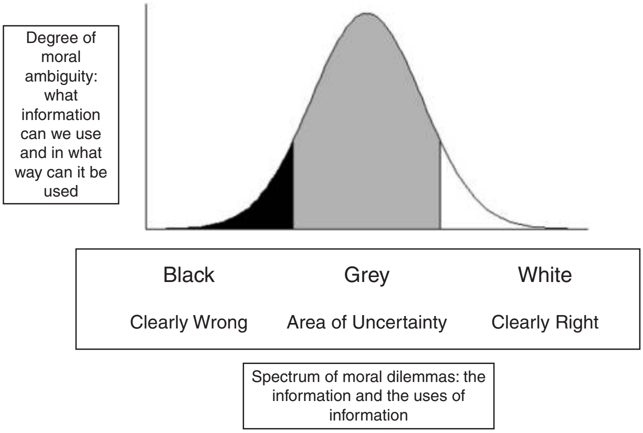
Degree of moral ambiguity: what information can we use and in what way can it be used
Black
Clearly Wrong
Grey
Area of Uncertainty
White
Clearly Right
Spectrum of moral dilemmas: the information and the uses of information

Figure 2.
Proportionate depiction of areas of moral ambiguity

There are five underlying rationales for business to develop a code of ethics. First, it can have a positive impact on the firm's relationship with its external stakeholders (in this case, data subjects who may be wary of sharing personal information). Second, such a code can positively impact the organizational members themselves. A good moral culture is more likely to produce satisfied internal constituents leading to better productivity. Codes can also be developed to assuage public concern about the legitimacy and ethical nature of management decisions – i.e., is the firm careful with personal information, does the firm exercise regard for the security of such information? Further, codes can be used to set the legal minimum behavior, the level below which the firm, its employees or others with whom the firm shares personal information, should not go. Finally, codes of conduct are developed to promote a higher moral standard to which all should aspire.

Next, we turn our attention to reviewing the ethical foundations of a possible code of ethics for data miners. Two deontological frameworks provide a sound basis for the conclusions that such codes are not only possible, but also desirable as statements of policy and of good faith on the part of the data miner. The Kantian (Kant, 1964) analysis and a study of Aristotelian virtues are particularly suitable as providing the basic moral precept to online privacy policies. These deontological analyses require recognition that there is a duty to act or not act aside from the consequences of the proposed action or inaction (the teleological approach to making moral decisions). Kant's categorical imperative provides the "first order moral principles," which, when used by persons in a rational frame of mind, provide guidance in the formation of "second order moral principles." Those second order moral principles dictate the appropriate policies for data mining and use. Not only does the decision maker have to be rational to utilize this approach, but there is a duty to act (or not) only if all the first order moral principles are satisfied.

There are three first order moral principles – the requirement that the actor treat all acted upon equally and in like manner to action he would accept, the requirement that the person acted upon is regarded as inherently valuable and not just viewed as a tool to attain the actor's own ends, and the requirement that freedom of the person acted upon is respected. The first requirement could be phrased as a question by the data miner – how would I want my personal information collected, stored online, and/or shared with others? For satisfaction of the second requirement, the question for the data miner might be whether the collection or use of the data could somehow benefit the data subject, rather than merely using him to satisfy some purpose only helpful to the data miner. Finally, the third requirement commands the data miner to acknowledge and respect autonomy of all rational beings. Specifically, the data miner should recognize the consumer's right to make a choices about the provision of data, as well as its use, storage, security, and the possibility of sharing with other data mining entities. The Kantian analysis has long been distilled to the Golden Rule – one should do unto others as he would have others do unto him.

The Aristotelian virtues (Aristotle, 1984; Bragues, 2006) also provide guidance in the building of the proposed ethics code. Six Aristotelian virtues are of merit for online privacy policies: courage, self-control, generosity, magnificence, sociability, and justice. Courage is the ability to regulate fear. It encompasses the ability to overcome apprehension and proceed with a business strategy in the face of risk, tempered primarily by the unwillingness to engage in illegal activities. It is within this framework that a data miner must evaluate the danger of consumer alienation or disfavor and the potential benefits of increased sales potential – mindful, however, of any legal limitations on such data collection and the ethics of sharing personal information without the data subject's knowledge or consent.

Self-control reflects data miners' attitudes toward pleasure and self-gratification. In a consumption-oriented society, both data miners and data subjects might succumb to excess. In the pursuit of the gratification associated with the disclosure, the data miner might inappropriately attempt to sell personal information about the data subject without first following proper protocol and conforming to required standards. In addition, data miners may demonstrate a lack of self-control by "entic [ing] others to vice" (Bragues, 2006, p. 347) – i.e., encouraging data subjects to reveal personal information by making it a requisite to completion of the transaction. Self-control of data subjects is implicated when, even knowing that too much personal information is being shared, a subject proceeds with disclosure in order to obtain the benefit of the deal.

Closely linked to self-control, the virtue of generosity is associated with the attainment and disposition of wealth. Failure to respect this virtue, and thereby succumbing to avarice, has negative implications for both the data miner and data subject, as the data miner might chose to take advantage of other data subject's vulnerabilities, i.e., the data subject's need and want to engage in online transactions. In so doing, the data miner may sacrifice his reputation for meager returns (Bragues, 2006). The data subject, on the other hand, can fail to meet the ideal of generosity by sharing too much information in an uninformed or careless way (Bragues, 2006). In either instance, there should be a median path that will suit the needs of each party.

Magnificence is closely related to the concept of generosity and implies the expenditure of large sums in the right way for a good reason. It is not defined or marked by displays of opulence, but rather the utilization of wealth in manner that benefits spender and community. Data miners could use the concept of magnificence to defend the amount of information sought or sold to a third party as being "reasonable," and beneficial to the facilitation of ease and convenience of the consumer experience.

Sociability is the idea that one should act pleasantly and professionally with others. Essential to maintaining a productive and satisfactory internal work environment, as well as sustainable customer relations, this attribute should permeate business in dealings regardless of the nature of those dealings. This virtue is especially important in the online services context. Data miners should provide an environment for data subjects wherein the data subject has a well-founded feeling that disclosure of personal information is less risky, safe, and reasonable in scope. Likewise, the data subject should be professional, yet reasonably amenable, when assessing the need to share personal information, as well as the extent to which that information can be comfortably shared.

Finally, although there are many levels to Aristotle's discussion of justice, in its most simplistic form, justice reflects the idea of proper allocations of goods. Aristotle believed that people should recognize the true value of exchanged items and that cultivation of such information is part of the process of developing and adhering to a code of ethics (Bragues, 2006). Underlying this belief is the notion that "a just person is thought to be someone inclined to obey the law and treat others fairly [. . .]" (Bragues, 2006, p. 349). Undeserved or unearned benefits should not be attained at the expense of others – each party to a transaction should get out the reasonable equivalent of what they put in. In the realm of data mining, justice can be applied through the proper allocation of benefits to the disclosing subject, taking into account the privacy level and volume of personal information provided, roughly equivalent to those derived by the mining company. Table II is a synthesis of philosophical attributes derived from the Kantian and Aristotelian perspectives aligned with their consequent guiding principles.

Methodology

The methodology that we used to craft foundational ethical principles for data mining and our proposed practices for online privacy policies for use in business followed several steps. After identifying the research questions, stakeholders were identified from various literature searches. As discussed earlier, identifying stakeholders is an important step to gain understanding of the effects of data mining; this analysis provides a very basic foundation, in a purely qualitative way, for an assessment of the benefits and costs of data mining. Payne and Landry (2005), Earp *et al.* (2002), Jackson (2002), and Baumer *et al.* (2004) all contributed stakeholders to the list developed and used in this analysis. Further, the authors used a survey of existing frameworks found in legislation and regulatory instruments to identify critically important elements of online privacy policies. These frameworks include the Malaysian Personal Data Protection Act, the United Kingdom Data Protection Act, EU Directives, Safe Harbor Principles, the Organization for Economic Co-Operation and Development

Philosophical rule	Guiding principle
Universally consistent actions	Sensitive information must be kept securely via technical and managerial means
Respect individuals as inherently valuable	Access should be granted to the data subject to check for/correct mistakes, incompleteness, timeliness of data
Respect autonomy of all rational beings	Consumers have a choice to provide or not to provide information and must consent to the sharing or use of the information
Courage	Information should be accurate, relevant, complete and time-appropriate
Self-control	Data miners should be legally, socially accountable for failures
Generosity	Only data subject-approved sharing of data should be allowed
Magnificence	Information should only be utilized for the purposes for which it was requested and/or approved
Sociability	Notice and awareness that information is being collected and used
Justice	All of the above speak to the virtue of justice

Table II. Philosophical and principle synthesis

(OECD) Fair Information Practice (FIP) Principles, and the US's Code of FIPs. In the development of the list of stakeholders and the derivation of the foundational principles of online privacy policies and proposed practices, keywords were identified as being relevant. For example, as can be seen in Table III (which follows the analysis of the frameworks), words such as fair, legal, integrity, and right were qualitatively chosen for their meanings and then identified in the various documents as being integral to the policy. Those words, taken in context, were fitted into our derived foundational principles and proposed practices for online privacy.

More issues: a comprehensive study on data mining policies

The Ponemon Institute (2006) compiled information in nine substantive areas by examining European and US corporate privacy practices. The first area relates to the existence of privacy policies, their content, and their uses. Communication and training questions concerning the ease of understanding of the policy, the process for communicating the policy to those affected, and the identification of appropriate training techniques for the firm's data handlers. Another area of review relates to privacy management. The questions here relate to management's role in establishing and implementing privacy policies. Data security methods, including the technologies used to secure data, privacy platforms and cookie use were surveyed. The sixth and seventh issues are privacy compliance and choice and consent.

The institute reviewed cross-national standard examination among businesses to see if the international element of data mining was important to the firms surveyed. The consumer's ability to redress problems encountered with privacy policies is addressed. Finally, the study looks at more procedural issues, including corporate budgeting to establish, implement, and control for privacy policy and issues, as well as the maturity of privacy policy efforts (i.e. has the firm just begun to examine data mining as a privacy issue for themselves and their consumers or have they been managing a privacy policy that addresses data mining for some time). The elements studied provide insight as to the concerns felt by business, consumers, and society. Drawing on all these perspectives, the authors of that study develop a "laundry list" of good questions any business, consumer or regulatory body could use to ascertain a firm's commitment to preserving data privacy.

Elements of a good privacy policy

Numerous authors adhere to the idea that the law and ethics are not necessarily the same thing. Many laws come from what society believes is ethical; for instance, our morality has dictated that there be a law preventing murder. However, not everything that is unethical is illegal. Cook and Cook (2003), Payne and Landry (2005), and van Wel and Royakkers (2004) all agree that legality does not necessarily translate into moral acceptability. Thus, while there are laws that regulate online privacy behaviors, it is imperative to go further – not only to protect individuals from an invasion of privacy, but also to allow businesses to continue to responsibly use data mining techniques to better serve the consuming public. The development, then, of a uniform code of online privacy ethics is, although grand in scale, merited:

> There is a manifest need for the negotiation of an international, technology-neutral, certifiable, management standard for the implementation of the information privacy principles that may be implemented by any public or private organization that collects, uses, processes or discloses personal information via the Internet, or through any other public or private network (Bennett, 2000).

Malaysia	UK	EU Directives	Safe harbor	OECD	FTC	Common concepts
Processing principle	Fair and legal processing	Prior permission to store and access personal data	Guarantee of data integrity	Collection limitation principle	Notice and awareness	Notice and awareness that information is being collected and used
Notice and choice principle	Maintain rights of data subject	Notice and choice	Notice Individual choice		Notice and awareness	
Security principle	Technical and organizational security protection measures	Confidentiality and security principle		Security principle	Security	Sensitive information must be kept securely via technical and managerial means
Notice and choice principle	Information should be adequate, relevant, not excessive	Information should be adequate, relevant, not excessive	Information should be accurate, relevant, complete	Data quality principle Openness principle	Choice/ consent	Consumers have a choice to provide or not to provide information and must consent to the sharing or use of the information
					Integrity	Information should be accurate, relevant, complete and time-appropriate
Retention principle	Retained with regard to timeliness	Retained with regard to timeliness				
Data integrity principle	Maintain rights of data subject	Respect rights of subjects		Purpose specification principle	Integrity	Information should only be utilized for the purposes for which it was requested and/or approved
Access principle		Right of access	Right of access	Individual participation principle	Access, participation	Access should be granted to the data subject to check for/correct mistakes, incompleteness, timeliness of data
Disclosure principle	Sharing limitations		Onward transfer principle	Use limitation principle		Only data subject-approved sharing of data should be allowed
	Specified, legal purposes		Enforcement	Accountability principle	Enforcement	Data miners should be legally, socially accountable for failures

Table III. Existing legislative and regulatory frameworks: finding their common concepts

In the realm specifically of web policies, the US government has offered suggestions as to some effective elements of a code, including the concept that disclosure should be clear and conspicuous and posted in a prominent location. Additionally, it should be readily accessible from the website's homepage or the page containing consumer information. To actually be of use to the consumer in making choices about sharing information, the US government further recommends that the notice be unavoidable to the consumer and easy to comprehend (Federal Trade Commission (FTC), 2012). Privacy principles have also been identified as being important internationally in the ISO/IEC 29100 standards. Language in this set of principles includes language and topics similar to other guidelines, including language related to consent and choice for the data subject, the purpose and legitimacy of the data collection and information on limitations of data collection practices. Further principles address issues related to the use, retention and disclosure of information, the accuracy and quality of the information collected and retained, individuals' participation in the data mining exercise and their access, as well as the accountability of those involved in data mining (International Standards Organization, 2011).

Jensen and Potts (2003, 2004) state that, if a business uses a privacy seal indicating that certain standards of privacy are adhered to, then the business should indeed adhere to those standards. The FTC (2012), in its Code of FIP, suggests a number of mechanisms for self-regulation and accountability in enforcing online privacy policies. For example, making it a condition of membership into a trade organization, utilizing external audits to verify compliance with the firm's own code, and certification programs that ensure that a firm is following best practices with regard to their data mining activities. In a sweeping review of many more legal frameworks than we have presented here, Greenleaf (2007) emphatically states that information privacy policies must be legally enforced, under the supervision of an independent body.

We reviewed a number of existing legal and regulatory frameworks to provide a baseline of what must be included in any effective practices related to online privacy. We used two primary criteria to determine which frameworks to examine in more detail. First, we wanted to ensure that the framework was both easily accessible and referenced in the extant literature. Second, we wanted the frameworks to span different countries, allowing a more broad-based look at the problem. Among those existing frameworks are both legal codes and voluntary, private-sector efforts to secure privacy for online consumers. These frameworks provide the basic elements of the comprehensive code of ethics for data mining privacy and integrity. Additionally, the basic elements identified have been utilized to develop a more detail-oriented set of proposed practices for businesses concerned with online privacy issues.

Framework 1: the Malaysian Personal Data Protection Act. Azmi's (2011) research centered on the Malaysian Personal Data Protection Act 2010. This law contains seven principles that can aid in the creation of a single code of ethics for business' online privacy policies. First, personal data are not to be processed without certain conditions being met. The collection and use of the data must have a lawful purpose directly related to the data subject's activities, must be necessary for, or directly related to, that purpose, and it must be adequate but not excessive relative to that purpose. Second, ensuring that a data subject's has effective notice that his information is being collected, and ascertaining whether it is his choice to accept such collection, are critically important elements to good process. Such notice and acceptance should be obtained in writing. The third principle relates to disclosure. It is the data subject's right that his information not be shared with other data miners or used for purposes other than that for which the information was originally collected, except in certain circumstances known to the data subject. Further, the data miner must take practical steps to assure protection of the data from loss, misuse, modification, unauthorized or accidental use, or disclosure, alteration or destruction. Fifth is the retention principle which dictates that personal data should only be kept for a reasonable time, until the completion of the purpose for which it was collected; thereafter, it should be destroyed. Data integrity is the basis of the sixth principle. This mandates that the data miner reasonably ensure that the personal data are accurate, complete, timely, and not misleading. Finally, the access principle requires the data subject to be given appropriate access to his information in order to make any corrections or additions needed to make the information accurate and timely.

Framework 2: the United Kingdom Data Protection Act. The UK has passed the United Kingdom Data Protection Act of 1998 (1998), citing eight principles relating to privacy and confidentiality. First, personal data should be processed fairly and lawfully. Second, it should be collected only for a specified legal purpose and should not be used for other purposes. Third, the personal data collected should be adequate, relevant, and reasonable in amount for the intended purposes for which it will be used. Accuracy and timeliness are also principles, along with is the idea that data should be kept only for a reasonable time to fulfill the purposes for which the information was collected. The sixth principle specifies that personal data should only be processed in accordance with the rights of the data subject. The law also mandates that appropriate measures be taken against the unauthorized or unlawful processing of the information, and/or accidental loss, destruction of, or damage to, the information. Finally, the law prohibits transfer of the personal data outside the European Economic Area, unless that country of destination has adequate protections in place to protect the data.

Framework 3: EU Directives. The EU mandates individual EU state behaviors through the issuance of directives. Directives regarding data mining have been developed. Central to these is the illegality of saving data without the data miner or storage agency first obtaining the data subject's consent (Carusi and Jirotka, 2009). Carusi and Jirotka extracted three principles from the EU Directives. First, the requirement that informed consent options be available. Second, that information collected should be "sanitized" to the greatest extent possible. And third, rules should be developed for accessing, tagging, or copying collected data. These are mandates that should be included in any and all online privacy policies. Other pertinent directives include the collection limitation principle, the openness principle and the individual participation principle (European Parliament, Council of the European Union, 1995).

The first principle, collection limitation, requires the fair collection of information, without resort to any kind of fraud, duress, or manipulation. The openness principle requires that the data subject be aware of the data collection and freely give consent. Additionally, this principle grants the data subject the right to know the details of the personal information collected and what, if any, of that information will be kept by the data miner. The remaining principle, the individual participation principle, allows the data subject to object to the use of his information. The targeting of suspect classification information, such as race or national origin, may not be collected unless this information is required for proper use of the data. Not surprisingly, security and confidentiality of personal information are also mandated, as is the notification of appropriate authorities as to the occurrence of data mining and its proposed use.

Framework 4: Safe Harbor Principles. Regan (2003) cites the seven principles of the "Draft International Safe Harbor Principles," noting that the issue of online privacy is, in fact, very much an international concern, not merely a domestic one. A "clear and conspicuous" notice on websites regarding the collection and use of personal information should be present. Individuals should be able to opt-out of specific uses of the information, and disclosures of the information to third parties should be optional. Subjects should also have the ability to access their own information to assure themselves that their personal information is accurate, relevant, and complete. The onward transfer principle mandates that organizations ensure that third parties to whom data access is given provide as much privacy as the original data miner. In addition, the guarantee of security, data integrity, and mechanisms for the enforcement of all of the provisions of the Safe Harbor Principles should be required.

Framework 5: OECD FIP principles. The Organization for Economic Co-Operation and Development (2011) developed a set of guidelines for data mining in 1980 and revisited them in 2011. The Organization recommends principles that are similar to the other provisions offered here. The collection limitation principle regulates the methodology with which data are collected – the data subject's knowledge and consent to have his information collected must be obtained. The data quality principle requires that personal data should be relevant, accurate, complete, and timely to the research purpose. The purpose specification principle requires that the data subject be informed, at the time the data are gathered, of the purpose of current and subsequent research for which it will be used. The use limitation principle prohibits the disclosure or use of personal information for purposes other than that for which it was originally collected. The security safeguards principle requires that collected data be protected against loss, destruction, and unauthorized access through the implementation of reasonable measures. The openness principle mandates that the data subject be clearly informed and freely accept the data miner's practices and policies in dealing with data. The individual participation principle allows individuals, at a reasonable cost and within a reasonable time, to know if someone has data about him and what that data are. Further, if the data subject's rights under this principle are denied, he has the right to challenge that denial. The accountability principle holds data miners accountable failure to comply with the principles of the OECD policy.

Framework 6: the code of FIPs. The US government has also addressed the issues surrounding data mining in the passage of the Code of FIPs (FTC, 2012; Electronic Privacy Information Center, 2012). This code, which is again similar to regulations in many jurisdictions, enumerates five principles. First, personal data record-keeping systems should not be kept secret. Notice that information is being collected must be made, including communication as to what is being collected, by whom, and for what purpose. Mechanisms must be in place to ascertain who may have access to the information. Finally under the first principle, the information must be given freely; if there are consequences for a subject failing to provide information, he must be alerted as to those possible consequences. Second, the data subject must be able to determine what of his information has been collected, stored, and used. There must be choice and consent on the part of the data subject. The data subject must also have access to the personal information held by others and the ability to correct inaccurate or incomplete holdings, in a timely, easy, and inexpensive manner.

Integrity and security of the data is the subject of the fourth principle. It dictates that data should be accurate and securely stored. The data miner is responsible for this, as well as for making sure that the data collected is correct and sufficient to be "good" information. The provisions of this principle envision technical and managerial efforts to assure compliance and to prevent loss, destruction, or unauthorized viewing of the data, as well as ensuring only prescribed uses. The final mandate of the federal provisions requires enforcement, including the right of the data subject to proper redress of grievances. Eight common concepts are presented in Table III as a summary of all the frameworks discussed, as well as a unification of the principles.

If we then examine the common concepts outlined in Table III and the legal, consumer/social, and business perceives described earlier, a comparison can be created that links these concepts as shown in Table IV. It is these unified principles that will form the basis of a uniform code for ethical data mining which should then drive the specific implementation of a privacy policy for a firm.

Through integration of the philosophical attributes set forth in Table IV and the policies set forth by Payne and Raiborn (2013), a set of proposed practices for online privacy policies has been developed as shown in Table V. These proposed practices take into account the legal, consumer and social, and business perspectives and is not solely focussed on one area. This is an important consideration in developing a policy that is not myopic and considers all aspects of data protection that are required by a variety of stakeholders. By categorizing each proposed practice by the overarching philosophical rule, they can then be utilized by practitioners in developing sound online privacy policies.

Discussion and implications

Comparing proposed practices to reality

In developing Table V, a question that arises is, does what is used in industry (practice) match the proposed best practices outlined in this paper? In reviewing a pseudo-random

Perspectives principle derived	Common concepts for an effective online privacy policy
Legal perspective Both the letter of the law and the spirit of the law must be observed	Sensitive information must be kept securely via technical and managerial means Only data subject-approved sharing of data should be allowed
Consumer/social perspective Consumers have rights and responsibilities with regard to the exercise of care, good faith, and competence in sharing personal information	Consumers have a choice to provide or not to provide information and must consent to the sharing or use of the information Information should be accurate, relevant, complete and time-appropriate Information should only be utilized for the purposes for which it was requested and/or approved Access should be granted to the data subject to check for/correct mistakes, incompleteness, timeliness of data
Business perspective Business have rights and responsibilities with regard to the exercise of care, good faith, and competence in the solicitation and uses of personal information	Notice and awareness that information is being collected and used Data miners should be legally, socially accountable for failures

Table IV. Comparison of perspectives principles and common concepts for an effective online privacy

Table V. Proposed practices for online privacy policies

Philosophical rule	Proposed practices for online privacy policies
Universally consistent actions	Comply with the letter of all applicable law, including providing notice, security, and data integrity, particularly with sensitive information Support legislation that allows for a reasonable system of information collection and sharing Support industry efforts to self-police, using the spirit of the law
Respect individuals as inherently valuable	Encourage data subjects to access their personal information to check for accuracy, relevance, comprehensiveness, and timeliness Support industry efforts to self-police, using the spirit of the law Encourage and engage in discussions about why people share personal information, what constitutes personal information Encourage firm and employee pride in self and community through clearly alerting data collectors and users as to their policies and adherence to same
Respect autonomy of all rational beings	Allow consumers to have a choice to provide or withhold information Use only truthful, candid privacy policies and notices regarding collection, storage, security and sharing of personal information
Courage	Encourage data collectors to pursue accuracy, relevancy, comprehensiveness, and time-sensitivity checks on all data collected Disclose all data collection practices Disclose state or country of domicile to all data subjects Encourage higher standards of ethics for all relevant trade associations Disclose financial relationships with those with whom data are shared
Self-control	Data miners should be legally and socially help accountable for failures regarding data privacy Encourage consumer responsibility about personal information provision Limit the data collection to that which is reasonable given the purposes for which the data are collected and that the data subject is aware Corporate culture of accountability of all stakeholders encourages accountability among employees/management
Generosity	Only share data with others whom the data subject has approved Craft alternative mechanisms by which those who do not want to share personal information can still do business online Support legislation that allows for a "reasonable" data collection and sharing
Magnificence	Only use data collected in the manner and with those allowed by the data subject Adjust security levels reflective of the sensitivity of the personal information provided Use appropriate and responsible data collection and sharing practices
Sociability	Provide notice of data collection/sharing Train employees to recognize and discourage provision of unnecessary or unnecessarily private personal information Provide a means by which customers can express negative experiences and make organizational recommendations on how to correct problems
Justice	Engage in consumer education about data mining, its purposes, consumer rights, etc. Limit the use of mechanisms that unfairly collect, store, manipulate, or share personal information

Source: Adapted from Payne and Raiborn (2013)

sample of different online privacy statements posted on the internet, it is very clear that some organizations do a better job than others. This review was performed by employing a Google search on the terms "Privacy Statements" or "Privacy Policies" and selecting different organizations. The organizations reviewed included telecommunication firms, technology companies, a US denominational church website, insurance companies, a school of business, financial companies, retailers, a spa, a hospital, and an airline. These organizations were selected in an attempt to provide a breadth of industries to investigate. The complete list of organizations can be found in Table VI.

In order to determine how well the privacy policies of these organizations align with our proposed practices, we employed the following analysis technique. Each privacy statement was reviewed used using the proposed practices concepts outlined in Table V as a rubric. For example, if a statement matched all three concepts under universally consistent actions then it received a fully meets, if it met some, then partially meets, and does not meet if none of the concepts were found. If there was uncertainty or the concept had to be inferred from the policy, then the firm's policy received the lower rating.

It is interesting to note that after reviewing 18 organization's online privacy policies that so many do not meet the proposed practices prescribed in Table V. All policies were found to be lacking in courage and most were lacking in the majority of the other categories as shown in Table VII. While the findings from a review of 18 policies is by no means representative of all online privacy statements, it is enlightening to see the

Table VI.
Online privacy statements reviewed

Company	Headquarters	Sector
AT&T	USA	Telecomm
Bemis Manufacturing Company	USA	Manufacturing
Comcast	USA	Telecomm
Facebook	USA	Social media
Fox Media	USA	News
Ikea	Sweden	Retail
J.P. Morgan	USA	Banking
Liberty Mutual Insurance	USA	Insurance
Morgan Hotel Group	USA	Hospitality
Pervasive Data Solutions	USA	Data management
Presbyterian Church USA	USA	Church
Queensland Government	Australia	Government
Spirit Airlines	USA	Travel
St Michael's Hospital	Canada	Hospital
The Wharton School, University of Pennsylvania	USA	Education
Wellchoice Matrimony	India	Dating/marriage services
Wellcome Trust	UK	Medical research
Woodhouse Spa	USA	Health and wellness

Table VII.
Summary of online privacy statements

Philosophical rule	Fully meets	Partially meets	Does not meet
Universally consistent actions		18	
Respect individuals as inherently valuable	1	1	16
Respect autonomy of all rational beings	3		15
Courage			18
Self-control		3	15
Generosity	2	2	14
Magnificence	2	2	14
Sociability		18	
Justice	1	8	9

various areas that are ripe for enhancement in practice. Table VII provides a glimpse at the philosophical rules that may be worth advocating more emphasis for as organizations refine their online privacy policies. These areas may also warrant further investigation with future empirical research concerning the current practices of organizations spanning different industries. It was encouraging to find that half of the policies examined made some attempt at educating the data subject on data mining purposes and threats (justice).

An amalgam of both the philosophical (Kant, 1964; Aristotle, 1984; Bragues, 2006) and the contemporary (i.e. EU Directives and Safe Harbor Principles) provides an appropriate foundation for the development of a code of ethical conduct for data mining professionals. Common to both approaches, and integral to balanced and morally sound practice, are the ideals of security, rational purpose, informed consent, consumer and collector responsibility, and accountability. Our suggestions support the use of data mining as the positive tool seemingly envisioned by Van Wel and Royakkers (2004), Jackson (2002), and Monash (2006). It further supports the notion that privacy is a negative, fundamental human right not to be interfered with (ISTPA, 2001; Pearson, 2009). The presentation of common concepts for online privacy policies and associated proposed practices provides a new "take" on existing principles: we have rooted our suggestions very firmly and clearly in well-respected philosophical thought. Policy makers mindful of fundamental ethical principles like respect, integrity, self-control, and justice may be more likely to efficaciously utilize those principles in the construction of further policies regarding data protection and online privacy.

The implementation and observance of a functional code of conduct for online privacy requires the full indoctrination of the supporting policies and practices by each and every stakeholder, data miner, and data subject. Indeed the sheer number and diversity of stakeholders demands a comprehensive code of ethics for online privacy (as found in, i.e. Payne and Landry, 2005; Earp *et al.*, 2002; Jackson, 2002). Each stakeholder has his personal ethics to consider, as well as the more standard edicts of professionalism. Data subjects are affected by adherence to codes of ethics or a failure of same, as potential benefit recipients or potential victims. Data miners are the reflected and reflexive recipient of benefit or harm: they benefit by the value they gain by increased business garnered as a result of ethical online policies and are harmed when stakeholders lose trust in their efforts to acknowledge and value ethical online privacy policies.

The development and implementation of a code of conduct as regards online privacy is also essential to ensure ongoing compliance with any existing local, state, and federal laws and regulations, as well as adaptation as these rules change and evolve to meet the growing utilization of the data mining process. Above all, it is imperative that each participant, whether data subject or data miner, be mindful of the fundamental privacy rights implicated by data mining. As Cook and Cook (2003) asserted customers expect businesses to anticipate their demands, as well as to meet their needs: engaging in data mining in an ethical way, a morally defensible way based on well-respected ethical principle, will allow business to anticipate and meet consumer demands, while respecting their right to privacy. This paper set out to answer three research questions regarding ethical online privacy policies:

RQ1. Are there common principles for online privacy policies and found three common perspectives emerge: legal, consumer/social, and business?

RQ2. If there are well-established ethical frameworks that firms can base their policies?

Key philosophical attributes were derived from the three perspectives and online policy principles. Lastly:

RQ3. What are some proposed practices for online privacy policies?

These are listed within the nine categories in Table V and can be used as a basis by any firm in determining their privacy policy.

The implications for business is that privacy concerns about online transactions are not going away and that there are moral and ethical standards that can be used as part of the development of online privacy policies. It should be noted that this paper has not focussed on the technical controls for ensuring confidentiality, availability, and integrity to protect data at rest, in motion, and in processing. Rather we have focussed on the ethical frameworks. This is an important distinction as the policy should drive the technical controls employed and not vice versa. However, this distinction is not limited to data mining and can be extended to numerous business processes. Additionally, it is important to consider all stakeholders involved in data collection, processing, and storage. Our research contributes to the stream of research in this area by providing a platform for discussion: the privacy codal provisions and the list of proposed best practices. The debate over privacy rights, particularly with regard to online transactions, is well-entrenched; to more effectively and efficiently provide online transactions, to more effectively and efficiently serve consumer and societal needs and to more effectively and efficiently conduct business, business and society must continue to define and refine policies dedicated to preserving the rights and abiding by the responsibilities of all stakeholders. This effort is aimed at aiding in this debate.

Limitations and future research

The limitations of the paper are clear: it is based in theory, rather than on empirical evidence. However, this is a limitation that gives rise to an opportunity. An opportunity for future research exists in the notion that our theoretically/qualitatively derived construct could be tested empirically: we can ask subjects their thoughts on codes that have been constructed using our proposed best practices as compared and contrasted with codes which have not. Depending on the results of those findings, we will have the opportunity to gauge whether our suggestions that codes of ethical conduct should be based in traditional notions of fair play and substantial justice as reflected from the Kantian and Aristotelian analyses. Two other avenues for future research include exploring in depth a particular industry or examining national differences in how organizations' current practices involving their online privacy policies align with the proposed practices presented here. Table VI provides a starting point for these avenues.

References

Alas, R. (2006), "Ethics in countries with different cultural dimensions", *Journal of Business Ethics*, Vol. 69 No. 3, pp. 237-247.

Aristotle (1984), "On virtues and vices", in Barnes, J. (Ed.), *The Complete Works of Aristotle, The Revised Oxford Translation*, Princeton University Press, Princeton, NJ, pp. 1982-1986.

Azmi, I.M. (2011), "Bioinformatics and genetic privacy: the impact of the Personal Data Protection Act of 2010", *Computer Law & Security Review*, Vol. 27 No. 4, pp. 394-401.

Baumer, D.L., Poindexter, J.C. and Earp, J.B. (2004), "Meaningful and meaningless choices in cyberspace", *Journal of Internet Law*, Vol. 7 No. 11, pp. 3-11.

Bennett, C. (2000), "An international standard for privacy protection: objections to the objections", *Proceedings from Computers, Freedom & Privacy 2000: Challenging the Assumptions*, Toronto, ON, available at: www.cfp2000.org/papers/bennett.pdf

Bragues, G. (2006), "Seek the good life, not money: the Aristotelian approach to business ethics", *Journal of Business Ethics*, Vol. 67 No. 4, pp. 341-357.

Carroll, A.B. (1979), "A three-dimensional conceptual model of corporate performance", *Academy of Management Review*, Vol. 4 No. 4, pp. 497-505.

Carusi, A. and Jirotka, M. (2009), "From data archive to ethical labyrinth", *Qualitative Research*, Vol. 9 No. 3, pp. 285-298.

Cook, J.S. and Cook, L.L. (2003), *Social, Ethical and Legal Issues of Data Mining*, Idea Group Publishing, Hershey, PA.

Cranor, L.F. (2005), "Giving notice: why privacy policies and security breach notifications aren't enough", *IEEE Communications Magazine*, Vol. 43 No. 8, pp. 18-19.

Culnan, M.J. and Bies, R.J. (2003), "Consumer privacy: balancing economics and justice considerations", *Journal of Social Issues*, Vol. 59 No. 2, pp. 323-342.

DeGeorge, R.T. (2010), *Business Ethics*, 7th ed., Pearson, Upper Saddle River, NJ.

Earp, J.B., Anton, A.I. and Jarvinen, O. (2002), "Social, technical and legal framework for privacy management and policies", *AMCIS 2002 Proceedings, Paper 89*, *December 31*, pp. 1-10, available at: http://aisel.aisnet.org/amcis2002/89 (accessed March 31, 2014).

Electronic Privacy Information Center (2012), "The code of fair information practices", available at: http://epic.org/privacy/consumer/code_fair_info.html (accessed April 18, 2014).

European Parliament, Council of the European Union (1995), "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data", Journal L281, November 23, pp. 31-50, available at: http://aspe.hhs.gov/datacncl/eudirect.htm#ART27 (accessed April 18, 2014).

Federal Trade Commission (FTC) (2012), "Fair information practice policies", available at: www.ftc.gov/reports/privacy3/fairinfo.shtm (accessed July 18, 2012).

Freeman, R.E. and Gilbert, D.E. (1988), *Corporate Strategy and the Search for Ethics*, Prentice Hall, Englewood Cliffs, NJ.

Fule, P. and Roddick, J.F. (2004), "Detecting privacy and ethical sensitivity in data mining results", in Estivill-Castro, V. (Ed.), *Twenty-Seventh Australasian Computer Science Conference, Conferences in Research Practice in Information Technology in Dunedin, New Zealand, Conferences in Research and Practice Information Technology*, Vol. 26, Australian Computer Society Inc., Sydney, pp. 1-8.

Greenleaf, G. (2007), "Asia-Pacific developments in information privacy law and its interpretation", available at: http://law.bepress.com/unswwps-flrps/art5/ (accessed April 18, 2014).

Gurses, S., Troncoso, C. and Diaz, C. (2011), "Engineering privacy by design", available at: www.cosic.esta.kuleuven.be/publications/article-1542.pdf (accessed March 23, 2015).

Hoffman, L. (2012), "Data mining meets city hall", *Communications of the ACM*, Vol. 55 No. 6, pp. 19-21.

Hofstede, G. (1980), *Culture's Consequences: International Differences in Work-Related Values*, Sage, Beverly Hills, CA.

International Security, Trust, and Privacy Alliance (2001), "ISTPA framework project", available at: http://emoglen.law.columbia.edu/LIS/archive/privacy-legis/ISTPA-FrameworkWhitePaper013101.pdf

International Standards Organization (2011), "The privacy principles, ISO/IEC 29100: 2011 (EN)", available at: www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-1:v1:en (accessed March 23, 2015).

Jackson, J. (2002), "Data mining: a conceptual overview", *Communications of the Association of Information Systems*, Vol. 8 No. 1, pp. 267-296.

Jain, Y.K., Yadav, V.K. and Panday, G.S. (2011), "An efficient association rule hiding algorithm for privacy preserving data mining", *International Journal on Computer Science and Engineering*, Vol. 3 No. 7, pp. 2792-2798.

Jensen, C. and Potts, C. (2003), "Privacy policies examined: fair warning or fair game?", GVU Center technical reports, Georgia Institute of Technology, Atlanta, GA, available at: https://smartech.gatech.edu/bitstream/handle/1853/3215/03-04.pdf?sequence=3; http://hdl.handle.net/1853/3215 (accessed March 31, 2014).

Jensen, C. and Potts, C. (2004), "Privacy policies as decision-making tools: an evaluation of online privacy notices", *CHI 2004, Vol. 6, Vienna, April 24-26*, pp. 471-478.

Joyner, B.E., Payne, D. and Raiborn, C. (2002), "Building values, business ethics, and corporate social responsibility into the developing organization", *Journal of Developmental Entrepreneurship*, Vol. 7 No. 1, pp. 113-131.

Kant, I. (1964), *Groundwork of the Metaphysics of Morals*, Harper & Row Publishers, Inc., New York, NY.

Ma, Z. (2010), "The SINS in business negotiations: explore the cross-cultural differences in business ethics between Canada and China", *Journal of Business Ethics*, Vol. 91 No. 1, pp. 123-135.

Monash, C.A. (2006), "Data mining ready for a comeback", *Computerworld*, September 11, p. 45.

Orentlicher, D. (2010), "Prescription data mining and the protection of patients' interests", *Journal of Law, Medicine and Ethics*, Vol. 38 No. 1, pp. 74-84.

Organization for Economic Co-operation and Development (2011), "Thirty years after: the OECD guidelines for privacy", available at: www.oecd.org/dataoecd/63/56/49710223.pdf (accessed April 18, 2014).

Payne, D. and Landry, B.J.L. (2005), "Similarities in business and IT professional ethics: the need for and development of a comprehensive code of ethics", *Journal of Business Ethics*, Vol. 62 No. 1, pp. 73-85.

Payne, D. and Raiborn, C. (2013), "The ethics of payday loan practices", *Ethics & Behavior*, Vol. 23 No. 2, pp. 117-132.

Payne, D. and Trumbach, C.C. (2009), "Data mining: proprietary rights, people and proposals", *Business Ethics: A European Review*, Vol. 18 No. 3, pp. 241-252.

Pearson, S. (2009), *Taking Account of Privacy When Designing Cloud and Computing Services*, HP Labs, Palo Alto, CA, March 9, pp. 1-10.

Ponemon Institute (2006), "Benchmark study of European and US corporate privacy practices", available at: www.whitecase.com/files/publication/1e7a69e0-49e9-478e-abc1-303e107c4dd7/presentation/publicationattachment/4a78432a-bd1f-4363-ab82-32fab1729a1e/benchmark_study_privacy_practices_updated.pdf (acccessed March 31, 2014).

Raiborn, C. and Payne, D. (1990), "Corporate codes of conduct: a collective conscience and continuum", *Journal of Business Ethics*, Vol. 9 No. 11, pp. 879-889.

Regan, P.M. (2003), "Safe harbor or free frontiers? Privacy and transborder data flows", *Journal of Social Issues*, Vol. 59 No. 2, pp. 263-282.

Schein, E.H. (1985), *Organizational Culture and Leadership*, Jossey-Bass, San Francisco, CA.

Stevens, J.M., Steensma, H.K., Harrison, D.A. and Cochran, P.L. (2005), "Symbolic or substantive document? The influence of ethics codes on financial executives' decisions", *Strategic Management Journal*, Vol. 26 No. 2, pp. 181-195.

Thibodeau, P. (2002), "Vermont opt-in rules spur suit", available at www.computerworld.com/s/article/68179/Vermont_Opt_in_Rules_Spur_Suit?pageNumber=2 (accessed April 18, 2014).

Tsai, J.Y., Egelman, S., Cranor, L. and Acquisti, A. (2011), "The effect of online privacy information on purchasing behavior: an experimental study", *Information Systems Research*, Vol. 22 No. 2, pp. 254-268.

United Kingdom Data Protection Act of 1998 (1998), *Part II: Rights of Data Subjects and Others*, available at: www.legislation.gov.uk/ukpga/1998/29/contents (accessed March 1, 2014).

Van Wel, L. and Royakkers, L. (2004), "Ethics issues in web data mining", *Ethics and Information Technology*, Vol. 6 Nos 129-140.

Velasquez, M.G. (1999), *Business Ethics: Cases and Concepts*, Prentice Hall, Upper Saddle River, NJ.

Ware, W. (2007), "Contemporary privacy issues: historical development", available at: http://ares.southernct.edu/organizations/rccs/oldsite/resources/research/comp_and_priv/ware/hist_dev.html#hist_dev (accessed April 18, 2014).

Watson, J. (2006), "Ethics for engineers falls in an unstructured gray zone", *IEEE Potentials*, Vol. 24 No. 4, pp. 14-16.

Wood-Harper, A.T., Corder, S., Wood, J.R.G. and Watson, H. (1996), "How we profess: the ethical systems analyst", *Association for Computing Machinery, Communications of the ACM*, Vol. 39 No. 3, pp. 69-77.

Further reading

Bennett, C.J. (2010), "An international standard for privacy protection: objections to the objections", presented at The Internet Law and Privacy Forum Meeting, San Francisco, CA, September 11-12, available at: www.ilpf.org/events/jurisdiction2/presentations/bennett_pr/ (accessed March 3, 2014).

About the authors

Matthew D. Dean is an Associate Professor in the School of Business at the University of Southern Maine. He teaches in the fields of management science, operations management, and statistical data analysis. The crux of his research involves developing modeling tools and methodologies for addressing complex management decision-making challenges. He has published in numerous journals, including *Journal of Applied Psychology*, *Operations Research*, *European Journal of Operational Research*, *Decision Support Systems*, and *Communications of the ACM*. Matthew D. Dean is the corresponding author and can be contacted at: matthew.dean1@maine.edu

Dinah M. Payne is a Professor of Management at the University of New Orleans. Her teaching and research interests are in business ethics, domestic, and international law and management. She has participated in many international teaching and learning experiences, including the UNO-Innsbruck Summer School and the Semester at Sea Program, among others. She has been awarded a number of teaching, research, and service awards. She has been published in many journals, including the *Journal of Business Ethics*, *Communications of the ACM*, *Labor Law Journal*, the *Journal of Corporate Accounting and Finance*, the *Journal of Developmental Entrepreneurship*, and *Global Focus*.

Brett J.L. Landry is the Ellis Endowed Chair of Technology Management, an Associate Professor, and the Director of the Center for Cybersecurity Education at the University of Dallas. Over the last 20 years, he has worked in the area of information security in the public and private sectors and has published numerous journal articles, conference proceedings, book chapters on IT, higher education, and cybersecurity. Landry also holds numerous industry security certifications such as Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), Certified Information Systems Auditor (CISA), and Certified in Risk and Information Systems Control (CRISC).