School of Informatics and Engineering
Flinders University • Adelaide • Australia

Technical Report SIE-06-001
February 2006

On the Ethical and Legal Implications of Data Mining

Kirsten Wahlstrom[1], John F. Roddick[2], Rick Sarre[3], Vladimir Estivill-Castro[4] and Denise deVries[2]

[1] School of Computer and Information Science,
University of South Australia, Mawson Lakes Campus,
Mawson Lakes, South Australia 5095, Australia.

[2] School of Informatics and Engineering,
Flinders University of South Australia,
Adelaide, South Australia 5001, Australia.

[3] School of Commerce,
University of South Australia, City West Campus,
Adelaide, South Australia 5001, Australia.

[4] School of Information and Communication Technology
Logan / Nathan /Gold Coast Campuses
Griffith University,
Brisbane 4111, Queensland, Australia.

Abstract

Ethics must be a condition of the world, like logic.
Ludwig Wittgenstein, 1889-1951.

The development of data mining is presenting significant ethical and social issues that must be addressed if the new technology is to widely accepted. This paper explores a range of these issues identifying in particular: privacy, data accuracy, database security, stereotyping, legal liability and the broader research dilemmas. Each issue is discussed and the implications for policy development are explored. The paper includes some consideration of possible solutions and suggests avenues for further investigation.

1 Introduction

To paraphrase Winograd (1992), we bring to our communities a tacit comprehension of right and wrong that makes social responsibility an intrinsic part of our culture. Our ethics are the moral principles we utilise to assert social responsibility and to perpetuate safe and just societies. Moreover, an important lesson from the industrial revolution was that the introduction of new technologies can have a profound effect on our ethical principles. Nowadays, we strive to adapt our ethics to concepts as diverse as gender issues in cyberspace (Herring 1994, Spender 1995) and the appropriate use of management information systems (Wagner 1994). The recent emergence of very large databases, and the associated automated data analysis tools, present yet another set of ethical challenges to consider.

Improvements in computing power and storage capacity has enabled organisations to develop data-rich information systems as part of their core business and as a result there has been an exponential growth in the amount of data stored. Data collection itself has progressed from the transcription of paper-based records via manual data-entry processes to the use of scanners, biometric devices, bar-code readers, smart cards, mobile phones (Location Data, GPS), smart dust, RFID tags (qv. (Cavoukian 2004)), web casting and Internet users' mouse clicks. This generation of data has in turn generated a need for new techniques and technologies that can transform these data into interesting and useful knowledge and information.

Data mining algorithms, commonly embedded in larger knowledge discovery processes and systems, are automated analytical tools that have recently experienced a rapid increase in use. They combine the disciplines of statistics, databases, machine learning and information visualisation to effect analyses of large and complex datasets. Their goal is to reveal previously unknown patterns and relationships in data and to present potentially interesting rules that might provide a useful insight and/or a competitive advantage. Data Mining and Knowledge Discovery tasks are broadly categorised into two categories: descriptive and predictive. Descriptive mining describes the general properties of the data stored in the database. Predictive mining draws inferences from the data in order to make predictions. Those inferences which satisfy user-defined criteria for certainty and interest are used to make *proactive knowledge-driven business*

decisions (Cavoukian 1998). This makes data mining algorithms powerful tools for analysis and prediction and are thus expected to become one of the most significant tools in the foreseeable future.

There are a variety of ways in which individuals generate computer data including credit card purchases, subscriptions, medical records, rentals, mail-order and on-line purchases, banking records, loyalty clubs and publicly-available or government records. When these data are merged and mined, they can infer a person's tastes, associations, credit information, income, health and political interests. Discovered patterns produce profiles of stereotypes that are used in crime prevention and marketing strategies as well as in government and commercial policy making. The individual or group is now often compared to the stereotype when engaging in a relationship with a government department, an insurance company, a financial institution or other commercial enterprise.

An examination of the associated ethical issues is thus increasingly appropriate, if not overdue. Furthermore, the legal implications attaching to these developments are equally important and require examination.

Although social and ethical issues have been identified as pertinent to data mining (Kantarcioglu et al. 2004, Rainsford & Roddick 1999) and there is a growing concern regarding the (ab)use of sensitive information (Boyens et al. 2002, Cavoukian 1998, Clarke 1997, 1999, Clifton et al. 2002, Clifton & Estivill-Castro 2002, Gehrke 2002, Rachels 1975, Sarre 2005), there has been relatively little interest in examining them in detail. However, Estivill-Castro *et al.*, discusses recent surveys regarding public opinion on personal privacy which show a raised level of concern about the use of private information (Estivill-Castro et al. 1999). As discussed by Fule & Roddick (2004), there is some justification for this concern – a 2001 survey in InfoWeek (Wilder & Soat 2001) found that over 20% of companies store data on their customers with information about medical profile, a similar amount store customer demographics with salary and credit information, and over 15% store information about their customers' legal history. With this increasing level of storage of personal information there is a greater risk that misleading, erroneous or even defamatory rules might be generated. To demonstrate the potentially misleading nature of data mining, Leinweber mined United Nations data combined with stock market data (Leinweber 1997). It was found that the best indicator for the S&P 500 Index was the estimated level of butter production in Bangladesh.

This paper provides a foundation for further investigation. It contributes an identification of the relevant issues, a discussion of their consequences and a consideration of potential policy solutions. The following section of the paper presents some of the key ethical issues. The first four subsections discuss privacy, data accuracy, database security and stereotypes. These issues have either arisen as a direct consequence of, or have immediate repercussions for, data mining practices. The next two sections investigate legal liability and the broader research dilemmas. Finally, a discussion of potential solutions is presented, with an identification of possibilities for further investigation closing the paper.

2 The issues

It should be clear that data mining itself is not ethically problematic. The ethical dilemmas arise when mining is executed over data of a personal nature. For example, mining manufacturing data is unlikely to lead to any consequences of a personally objectionable nature. However, mining a clickstream of data obtained from an oblivious Internet user instigates a variety of ethical problems. Perhaps the most immediately apparent of these is the invasion of privacy.

2.1 Privacy

Complete privacy is not an inherent part of any society (Gavison 1984, Vedder 1999). This is because participation in a society necessitates communication and negotiation, which renders absolute privacy unattainable. Hence, an individual member of a society develops an independent and unique perception of their own privacy (Rachels 1975, Tavani 1999*b*). This being the case, privacy exists within a society only because it exists as a perception of the society's members. This perception is crucial as it partly determines whether, and to what extent, a person's privacy has been violated.

An individual can maintain their privacy by limiting their accessibility to others (Gavison 1984). In some contexts, this is best achieved by restricting the availability of their personal information. If a person considers the type and amount of information known about them to be inappropriate, then they perceive their privacy to be at risk. Thus, privacy can be violated when information concerning an individual is obtained, used, or disseminated, especially if this occurs without their knowledge or consent.

The use of different types of data and the context in which it is used inspires public debate over privacy and security issues. The use of medical and pharmaceutical records, and banking transactions for data mining is perceived by many to be more intrusive of an individual's privacy than data about their lifestyle and tastes.

In 1980, the Organisation of Economic Cooperation and Development (OECD) produced a set of guidelines (OECD 1980) for the protection of personal data. These guidelines acknowledge and encourage the individual's prerogative to control their personal information. One of the guidelines states that the reason for collecting personal data should be made clear to the individual prior to collecting it and another that data cannot be used for any purpose other than that stated when the data were obtained. Data mining potentially violates both of these principles.

First, it is impossible to define accurately the purpose of a data mining exercise as it is intrinsically related to the information it discovers. Second, and more importantly, data mining is conventionally executed over large amounts of historical data and thus uses data collected for one purpose for another purpose. Third, the information revealed during data mining may be considered inappropriate (in terms of type and quantity) by the individuals whom it concerns. These violations diminish the individual's ca-

pacity to determine which, and how much, personal information is known about them, and thus threatens to violate their sense of privacy.

Huge volumes of detailed personal data are regularly collected and analysed by marketing applications using data mining (Berry & Linoff 1997, Bigus 1996, Peacock 1998, Khaw & Lee 1995) and various commercial applications, in which individuals may be unaware of the *behind-the-scenes* use of data mining, are now well documented (John 1999, Klang 2004). However, privacy advocates face opposition in their push for legislation restricting the secondary use of personal data, since analysing such data brings collective benefit in many contexts (Gordon & Williams 1997). Data mining has been instrumental, for example, in many scientific areas such as biological and climate-change research and is also being used in other domains where privacy issues are relegated in the light of perceptions of a common good. These include human genome research (qv. (Tavani 2004)), combating tax evasion and aiding in criminal investigations (Berry & Linoff 1997) and in medicine (Roddick et al. 2003). Williams, for example, describes the use of mining techniques in studies in health care, taxation and insurance towards the collective benefit of identifying fraud, addressing compliance, and improving the delivery of health care (Williams 1999).

As privacy is a matter of individual perception, an infallible and universal solution to this dichotomy is not possible. What is an acceptable solution for one person may be insufficient or unacceptable for another. However, there are measures that can be undertaken to enhance privacy protection. Cavoukian suggests that individuals must be made aware that the information they provide is to be used for data mining and that they be given an opportunity to permit or deny access to their data (Cavoukian 1998). Current practices fall well short of this ideal. Commonly, an individual must adopt a proactive and assertive attitude in order to maintain their privacy, usually having to initiate communication with the holders of their data to apply any restrictions they consider appropriate. For the most part, individuals are unaware of the extent of the personal information stored by governments, private corporations and firms regarding, for example, credit ratings and other sensitive data. It is only when things go wrong that individuals exercise their rights to obtain this information and seek to excise or correct it.

Article 17 of the United Nations International Covenant on Civil and Political Rights 1966 (ICCPR) (UNHCHR 1966) defines the right to privacy and reputation.

1. *No one shall be subjected to arbitrary or unlawful interference with his* [sic] *privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*

2. *Everyone has the right to the protection of the law against such interference or attacks.*

Thus, any state which is a signatory to the covenant has a responsibility to identify and apply methods of privacy protection. Of course, not all countries are signatories to the ICCPR, and those which are may not be as diligent in seeking to enforce their responsibilities.

2.2 Data accuracy

The previous subsection noted the UN's commitment (UNHCHR 1966) to an individual's reputation and the OECD's guidelines (OECD 1980) for protecting personal data. Another of the OECD's guidelines requires personal data to be precise, complete and current in order to protect people from the harmful repercussions associated with poor data quality. This becomes more relevant when a data mining application reveals information that could have detrimental repercussions for a data subject, especially as information is customarily regarded as infallible (Gavison 1984).

Mining applications involve vast amounts of data, which are likely to have originated from many diverse, possibly external, sources. Thus the initial quality of the data cannot be assured and may be noisy, obsolete, inaccurate or incomplete (Cavoukian 1998). Moreover, although data pre-processing (or cleaning) is undertaken before the execution of a mining application to improve data quality, people conduct transactions in a sporadic and largely unpredictable manner, which can cause personal data to expire rapidly. In some cases, what is accurate data at one point in time is inaccurate shortly after that. When mining is executed over expired data inaccurate patterns are more likely to be revealed, which can lead to negative consequences for an individual specifically and groups and society in general.

Likewise, there is a great likelihood of errors caused by repetitive mining over poor quality data (Cavoukian 1998). This increases the threat to the data subject and the costs associated with the identification and correction of the inaccuracies. Thus, when mining is repeatedly executed over personal data, frequent cleansing and updating efforts are appropriate.

Moreover, the fact that data is commonly collected and analysed without a preconceived hypothesis shows that the data analysis used in data mining and knowledge discovery are more likely to be exploratory (as opposed to the confirmatory data analysis exemplified by many statistical procedures and techniques). This immediately implies that results from data mining algorithms require further confirmation and/or validation. That is, data mining results are (merely) suggested hypotheses for further confirmatory data analysis. There is a serious danger of inaccuracies that cannot be attributed to the algorithms, but to their exploratory nature.

This has caused some debate amongst the data mining community itself. For example, Freitas (2000) has argued that mining association rules is a deterministic problem which is directly dependent on the input set of transactions. He argues that the association rules are not to be used for prediction, as would be the case of learning classifiers where the input is considered a representative sample and the learner aims to minimise the error in further unseen examples. However, most uses of association rule mining are for extrapolation to the future, for some sort of prediction, and not just to describe the past.

2.3 Database security

In an ethical sense, database security is closely related to privacy. This is because database security inhibits the unauthorised dissemination of personal data thus further enhancing, albeit indirectly, an individual's capacity to regulate access to their data.

> *When data can be viewed from many different angles and at different abstraction levels, it threatens the goal of protecting data security and guarding against the invasion of privacy. It is important to study when knowledge discovery may lead to an invasion of privacy, and what security measures can be developed for preventing the disclosure of sensitive information (Chen et al. 1996).*

The development of data warehouses has increased the importance of database security. Prior to this, data were typically held in separate databases to which access was controlled and limited to people with a specific functional role. Data warehouses bring together data from multiple sources and therefore more complex factors need to be considered when establishing security measures.

In terms of database security, two forms of mining operation need to be considered:

1. Those operating as authorised applications by an individual or organisation that owns and has full access to the data;
2. Those operating as unauthorised applications by an individual or organisation that has access to the data only insomuch as has been permitted for other allowable purposes.

Note that an individual need not be external to the organisation that owns the data for the second point to occur.

Conventional database security protects data via user authorisation techniques (O'Leary 1991) making no distinction between the degrees of sensitivity present in the database (Mills 1997). A more sophisticated model, Multi Level Security (MLS), extends conventional security measures by classifying data according to its confidentiality (Elmasri & Navathe 2004). The data in an MLS database is typically sorted into four security levels, with users permitted access only to their authorised level. This increases the protection of data from misuse by both authorised users and intruders. Furthermore, encryption and auditing can provide additional levels of database security.

Miller (1991) showed how users executing specific queries at their authorised security level could easily infer more sensitive information. More recently, Thuraisingham (1997) discussed the possibility of this occurring during a data mining exercise. Moreover, while auditing can be used to identify offending users, a means of preventing unauthorised mining applications is still necessary.

One set of precautions that can enhance existing database security to improve the protection of personal data from unauthorised mining applications is outlined below. Firstly, inference to more sensitive data from less sensitive data can be partially inhibited by restricting mining applications to one security level (Lin et al. 1996). Secondly, the introduction of noise to the data can serve to corrupt the results of any symbolic learning techniques present in a data mining tool (Miller 1991, O'Leary 1991). Finally, the introduction of instability to the data (O'Leary 1991) renders it unsuitable for mining and hinders the extraction of potential meaningful information. The combination of these precautions within an MLS database security model can discourage unauthorised data mining by rendering it a complex and cost intensive exercise.

The security of data has been developed, in the main, to protect the assets of an organisation. The information held has value and security measures are taken to maintain the value. The interests of the individual, whose personal information is stored, are not taken into account unless it is deemed that a security breach would result in damage to the organisation. For example, loss of company reputation, legal repercussions or loss of market share.

Clifton & Marks (1996) identify security implications with the sharing of corporate data for data mining. The sharing of data may be cost-efficient and beneficial to organisations in a relationship but allowing full access to a database for data mining may have detrimental results. The adequacy of traditional database security controls are suspect because of the nature of inference. Private and confidential information can be inferred from public information.

An example is given of how names of individuals within an *unknown* project may be inferred from a publicly known telephone directory if those numbers are allocated sequentially within groups. Knowledge of an identifier assignment process is not necessary, if a rule can be found that clusters a group of people for a project by an identifiable attribute.

They suggest the following measures to prevent unauthorised mining:

- Limiting access to the data. By controlling access to the data and preventing users from obtaining a sufficient amount of data, consequent mining will not result in high confidence levels. This also includes query restriction, which attempts to detect when statistical compromise might be possible through the combination of queries (Miller 1991, Miller & Seberry 1989).
- Anonymisation. Any identifying attributes are removed from the source dataset. A variation on this can be a filter applied to the ruleset to suppress rules containing identifying attributes.
- Dynamic Sampling. Reducing the size of the available data set by selecting a different set of source tuples for each query.
- Authority control and cryptographic techniques. Such techniques effectively hide data from unauthorised access but do not prohibit inappropriate use by authorised (or naive) users (Pinkas 2002).
- Data perturbation. Altering the data, by forcing aggregation or slightly altering data values, useful mining may be prevented while still enabling the planned use of the data. For example,Agrawal & Srikant (2000) explored the feasibility of privacy-preserving data mining by using

techniques to perturb sensitive values in data. Two techniques presented are:

  - Value-class membership – where values for an attribute are partitioned into a set of disjoint mutually exclusive classes, in particular discretization.
  - Value distortion – which returns a value $x_i + r$ instead of x_i where r is a random value which may be calculated from either a uniform random distribution or a Gaussian random distribution.

- Data swapping. Attribute values are interchanged in a way that maintains the results of statistical queries (Evfimievski et al. 2002).
- The elimination of unnecessary groupings. By assigning unique identifiers randomly; they serve only as unique identifiers. This prevents meaningful groupings based on these identifiers yet does not detract from their intended purpose.
- Data augmentation. By adding to the data in non-obvious ways, without altering their usefulness, reconstruction of original data can be prevented.
- Alerting. Labelling potentially sensitive attributes and attribute values and from this calculating an estimate of the sensitivity of a rule (Fule & Roddick 2004).
- Auditing. The use of auditing does not enforce controls, but it may detect misuse so that appropriate action may be taken.

Issues relating to the computational cost of privacy preservation are discussed by Agrawal et al. (2004).

2.4 Stereotyping

Patterns discovered in data mining are used to build profiles of characteristics or behaviour. Analysis of the data held within databases may show certain buying patterns, social contact patterns or financial decision patterns which appear to be associated with particular groups. These are commonly generalised rules which, as Han et al. (1996) point out, reflect a general fact in the current database state. They do not enforce a constraint on all possible database states. That is, the profile produced is that of a hypothetical individual for which not a single real person need exist.

Custers (2003) points out that as one of the main applications of group profiles is selection, it follows that most of the disadvantages of using group profiles are closely connected to their advantages. As in non-distributive profiles not every group member has the group characteristic and there are different consequences depending on whether the characteristic is regarded as negative or positive. Custers describes four categories of people within group profiles (A) those that are in the negative group and have the negative characteristic, (B) those that are in the negative group but do not have the negative characteristic, (C) those that are in the positive group and have the positive characteristic, and (D) those that are in the positive group but do not have the characteristic. Not only are individuals advantaged or disadvantaged dependent upon which group they fit into, the people in categories B and D are treated incorrectly.

This aspect of profiling is not always recognised when it is used by marketing companies, financial institutions, insurance companies and police to categorise individuals. Services and treatment that people receive from these organisations is becoming more dependent upon how they fit a particular pattern than on a person-to-person relationship. Schreuders & van Kralingen (1998) warn that the production and use of *virtual identities* for categories of people is increasingly shifting attention from the attributes of an individual to those of the group. *Individuals will more often be judged and dealt with on the basis of the attributes of the group to which they (in many cases, by chance) belong rather than on the basis of their own particular characteristics and merits.* This practice has the potential of creating a new form of discrimination, the impact of which is more closely related to the ethics of the owner of the discovered knowledge than to society in general.

The use to which these patterns and profiles are put in a commercial environment can be seen in the following examples.

Stevens reported that an educational loan association hopes to use its database of 12 million current and previous student loan holders to become a database marketer. The company's director of customer resource management and digital intelligence stated that:

> *Using the database, the company can know, for example, when students graduate, when they pay off their loans, where they live, how often they change their address and whether they tend to pay their bills on time. All that information can be used to determine when they're likely to purchase a car, refinance their mortgage or sign up for long-distance service, or whether they'd be a good risk for a credit card. (Stevens 2001)*

They have entered into business relationships with a number of partners to sell long-distance services, auto insurance and financial products by direct mail and other marketing campaigns. Rindfleisch (1997) states that some secondary uses of data are in conflict.

> *For example, self-insuring employers, under the Employment Retirement Income Security Act (ERISA), are entitled to receive fully identified patient information for employees being covered. Such information is nominally used to help the employer/insurer make sound benefits management decisions, but it can also affect whether employees get promoted, or even whether their employment is continued.*
>
> *Once sensitive information about an individual is exposed and the resulting damage is done to that person, the information cannot be withdrawn and made secret again.*

Evans, in an article about banks and their use of Customer Relations Management (CRM) software, wrote

In their vision of a CRM-ruled future, consumers will bank almost entirely via phone and the Internet. What branches remain will operate like car dealerships, staffed by "sales reps", not tellers. This new breed of bank employee will get a commission for each mortgage, loan or investment portfolio landed with a profitable customer.

Sales reps will spot these profitable customers using CRM software to analyze an array of factors, including the customer's salary, age, marital status, debt, number of job and residence changes, education and property owned. Customers will be required to supply the data to open an account.

Customers identified as losers by CRM might get checking accounts - at a price. ... Unprofitable customers will pay an additional price in terms of service – (Evans 1999)

Oracle Corp., a leading Internet consultant for financial institutions, suggests collecting more than demographic and geographic data about customers. It recommends a CRM that warehouses "psychographic" data: hobbies, political opinions, magazine subscriptions and "actions", including clubs joined, recent purchases, restaurants and designer boutiques frequented. This allows financial institutions that own unrelated businesses to market these ancillary services as well.

A dilemma arises when a person lives in a less-desirable suburb, drives an older car and does no on-line or mail-order shopping. He or she could be more solvent, more financially responsible and, a better credit risk, but because a company's consumer profiling software did not give him/her a high ranking, it will not provide the same level of service or access.

A software system developed by the Vancouver Police Department (Rigel) is used to provide profiles giving:

- information about what crimes an unknown offender is likely to have committed;
- an insight into his/her characteristics and personality traits; and
- where the probable offender (using geographic profiling) is likely to be found.

Such technological support for criminal investigations and crime prevention is, in general, beneficial to society, however, how is an individual treated if he or she lives in a designated area and has habits and/or characteristics that match a criminal profile?

Clarke (1999) warns that a danger apparent in the context of location and tracking technologies is *... a vast increase in "circumstantial evidence" for criminal cases, which might dramatically affect the existing balance, including the presumption of innocence, and hence increase the incidence of wrongful convictions. This would in turn result in a more credible threat of conviction (including in ambiguous and spurious instances), and hence in increased repression of human behaviour.*

3 Legal Liability and the Research Dilemma

3.1 Legal Context

To this point, we have discussed ethical issues in the specific context of data mining. We now discuss the issue of the potential legal consequences attached to the practice of data mining.

When personal data have been collected it is generally decontextualised and separated from the individual, improving privacy but making misuse and mistakes more likely (Gammack & Goulding 1999). Recently, there has been an emerging trend to use personal data as a resource and offer it for sale. Information is easy to copy and re-sell many times. The phrase *data mining* uses the metaphor of the exploitation of natural resources, further contributing to the perception of *data as commodity*. Moreover, the question of whether it is appropriate in terms of human rights to trade in personal data has seen insufficient academic and legal debate. The negative consequences of such trade are similar to those of data mining: transgression of privacy and the negative impacts of inaccurate data. However, the repercussions of inaccurate data are more serious for organisations trading in personal data, as the possibility of legal liability is introduced. There is the potential for those practising data trade or data mining to make mistakes and as a consequence lose heavily in the courts.

Compensation (ie. *damages*) may be ordered by the courts against any organisation that is found to have harmed (or failed to prevent harm to) an individual to whom it owed a duty of care. In other words, once liability (in what is known as the *tort of negligence*) has been established, the plaintiff can claim financial compensation for any consequential losses caused by the negligent act (Samuelson 1993). The extent and exact nature of the losses (which may include pain and suffering) is, for the most part, unique to each plaintiff, but the boundaries of negligence are never closed. For example, a data mining exercise might erroneously declare an individual a poor credit risk, and decisions may be made prejudicial to that individual on the basis of that risk.

Note that in some cases, data mining algorithms may classify correctly, but such classification could be on the basis of controversial (ie. ethically sensitive) attributes such as sex, race, religion or sexual orientation. If used, a denial of credit based on race would have the same structure in a decision tree as the classification for teenagers as more at-risk motorists (with the associated higher insurance premiums). The latter is discrimination based on age that is regarded as acceptable. In some cases, such as artificial neural networks, support vector machines and nearest neighbour classifiers, which do not make their knowledge explicit in rules, the use of controversial classification attributes may be hard to identify. Even with methods that make transparent their classification, such as decision trees, there is little to prevent a corporation using rules based on controversial attributes if that improves accuracy of the classification. Individuals who suffer denial of credit or employment on the basis of race, sex, ethnic background or other controversial attributes in a context where this is contrary to law are in a strong position to demonstrate harm *only* if they illustrate the artificial classifiers are us-

ing such attributes. The question is how they obtain access to the classifier results.

In the event that the person loses money or reputation as a result of this mistake, courts may award damages. Moreover, since the potential for inaccuracies involved in the data mining exercise is great, it is conceivable that the courts might apply a higher than usual standard of care in considering whether an organisation has breached its duty to a plaintiff sufficiently to amount to negligence. Only time will tell.

Web-usage mining within a corporation is also controversial (Tavani 1999*a*, Van Wel & Royakkers 2004). Monitoring employees' use of the Internet has already been used for dismissal on the basis of inappropriate behaviour at work. Privacy advocates have had a hard time arguing in favour of individual employees against the duty of the corporation to ensure an environment free of threats such as electronic harassment. Parallels have been drawn between monitoring and web-usage mining as a deterrent of Internet abuse and surveillance cameras as deterrent of physical attacks. Broder (1999) reports on an active battle between web miners (who are hungry for personalised data) and privacy advocates (who object to the facilitation of monitoring and tracking technologies for visits to web sites). The conflict is in need of technology that can achieve balance.

Another legal issue which needs to be considered is whether organisations manipulating personal data can be considered capable of defaming a person whose data they have mined. It is quite conceivable that since data mining generates previously unknown information, the organisation using the data mining tool can be considered the author of the information for the purposes of defamation law. In addition, it can be argued that organisations trading in personal data are analogous to publishers, as they are issuing collections of data for sale and distribution. Hence, if the information is capable of being deemed defamatory by the courts, the data mining organisations are capable of being found liable for damages in this tort also. One difficulty is that the terms *author* and *publisher* have long been associated with text or music, not data. Note, however, that census data faces this challenge and other technologies are complicating the issue still further. Consider, for example, aerial/satellite photography that can now achieve resolution to within a few metres and which can be freely purchased over the Internet. What is the resolution that makes such data be considered personal data? How can individuals living at identifiable houses decide if the aerial photo is to be used for a potential beneficial analysis, such as bush fire risk analyses of their property, or an analysis that could be considered defamatory or discriminatory?

Market analysts often see privacy concerns as unreasonable. Privacy is an obstacle to understanding customers and to supplying better suited products (Culnan 1993). Hundreds of millions of personal records are sold annually in the US by 200 superbureaux to direct marketers, private individuals, investigators, and government agencies (Laudon 1996). In a more extreme example, the public good to be derived from mining medical data is considerable but the legal policy allowing or disallowing such use is equally complex (Saul 2001).

We are in urgent need of an extended interpretation of existing tort doctrine, or preferably a broadening of the boundaries of the current doctrines. Indeed, Samuelson (1993) warns that the engineered, technological nature of electronic information dissemination suggests a greater liability for its disseminators. Usually, the conveyers of information are excused from liability if they are simply the carriers of the information from the publishers to the public. For example, a book store selling a book that carries defamatory material will be excused from liability that might rightly attach to the author and the publisher. It is quite possible that a data mining exercise, particularly one that had mined inaccurate data, might be deemed by the courts to be an exercise in publishing, not just in dissemination.

3.2 Broader research dilemmas

When conducting research, well documented and clearly defined ethical guidelines should be followed by those interested in the integrity of their work. One example of such guidelines is the Australian *Joint NHMRC/AVCC Statement and Guidelines on Research Practice* (NHMRC/AVCC 1997)[1]. This document presents ethical strategies for data storage and retention, authorship, publication, supervision of students and research trainees, disclosure of potential conflicts of interest and research misconduct. It is intended to provide a national basis for Australian research institutions' ethics policies. Accordingly, research policies in universities and other research organisations cover human research procedures, genetic manipulation/recombinant DNA research, animal experimentation, radiation safety, biohazards and responsible research practice[2]. However, while these documents thoroughly consider the practical issues immediately associated with research, they fail to consider the sociological influence of research results generally and new information technologies in particular.

The term *disruptive technologies* has been coined by business researchers (Christensen 1997) to refer to technologies that have an agitating effect on a market and the organisations competing within it. How is it that this term has not been adopted by sociologists and computer scientists to describe technologies that disrupt our cultures? Examples of such technologies abound; a perusal of any computer ethics text (qv. (Baase 1997, Johnson & Nissenbaum 1995)) will reveal discourse regarding software accidents, risks, crime, hacking and so on. However, these discussions typically cite documented incidents and fail to identify the possibility of evaluating a technology's potential for social disruption[3].

[1] Similar guidelines exist in almost all Western countries, such as the USA Code of Federal Regulations, Federal Policy for the Protection of Human Subjects (Basic DHHS Policy for Protection of Human Research Subjects), the European Parliament directive 95/46/EC, and the ICC/ESOMAR International Code of Marketing and Social Research Practices.

[2] A useful interpretation of these guidelines in the context of computer science research in Australia has been released by *Computer Research and Education Association* (CORE) at `http://www.core.edu.au/conduct.html`.

[3] Albert Einstein lamented the impact of his research on humanity:

The previous section noted the pertinence of capacity when determining responsibility. While computer scientists' understanding of their work provides them with the capacity to argue on the work's behalf, it does not provide the capacity to estimate the work's social impact. Only a combination of suitably qualified individuals, historical information and a comprehensive understanding of the emerging technology can adequately provide such an estimate.

4 Potential Solutions

This paper has made the distinction between those ethical issues associated specifically with data mining and those of a more general applicability. It has also reviewed some of the legal consequences of the practice. These issues are now reviewed in order to discuss a range of possible policy solutions.

4.1 Specific solutions

4.1.1 Anonymisation of Data.

One solution to the invasion of privacy problem is the anonymisation of personal data (Clarke 1997). This has the effect of providing some level of privacy protection for data subjects. However, this would render obsolete legitimate data mining applications that are dependent on identifiable data subjects, and prevent many mining activities altogether. An abolitionist policy is, we contend, inappropriate.

A suggested compromise is the empowerment of individuals to dictate the amount and type of personal data they consider appropriate for an organisation to mine. Cavoukian (1998) suggests a two-option approach to this empowerment, where the organisation capturing the data provides the individual with the opportunity to permit or deny the use of their data for other purposes. These other purposes (for example, proposed data mining or data trade) could be identified and described, enabling informed decision-making on the part of the individual.

While anonymisation of data is a step in the right direction, it is the weakest of the possible options. It is well known that additional information about an individual can easily be used to obtain other attributes. For example, an anonymous table of salaries and addresses, together with the knowledge of one attribute would be sufficient to determine the other. In addition, grouping two sets of anonymised information can result in disclosure. Identifier removal (such as name, address, phone number and social security number) can be insufficient to ensure privacy (Adam & Wortmann 1989, Klösgen 1995). Anonymisation is a form of cell suppression, a technique applied on statistical databases. Indeed, the research agenda is still far from closed since most of the solutions proposed so far in the data mining community (Piatetsky-Shapiro 1995) are easily translated to previously suggested methods for statistical databases. The techniques in statistical databases are summarised in Table 1.

> *The release of atom power has changed everything except our way of thinking...the solution to this problem lies in the heart of mankind. If only I had known, I should have become a watchmaker.*

Weizenbaum (1972) later discussed the responsibility of the computer scientist to his/her society.

The solutions of the data mining community map to these statistical techniques as follows.

- Evaluating queries on the basis of a random sample of the data instead of the data itself maps to random sampling techniques. This method is particularly suitable for large data sets such as a census, but like the output perturbation techniques, suffers from partial disclosure and low consistency (Denning 1980). Moreover, providing a small enough sample so that mining techniques cannot find patterns (Clifton 1999) does not protect information privacy for those included in the sample, prevents finding useful patterns for beneficial uses of mining and can be compromised by acquiring several samples.

- Aggregating data by combining individual records with similar properties into atomic groups maps to partitioning; and thus, it may obscure important patterns (Shoshani 1997).

- Generating synthetic data with general patterns as original data maps to PDDP (Table 1). Distributions of variables are calculated on the bases of the original data set, and a new data set is drawn as a sample from those distributions (Klösgen 1995). For a large number of variables, data generation becomes difficult (Piatetsky-Shapiro 1995). In addition, if data are generated by some probabilistic model, we may as well release the model since this is the most machine learning methods would learn. Thus, this approach blocks methods for learning beneficial collective patterns.

- Relying on limitations of rule induction techniques (O'Leary 1991) (for example, their capacity to handle noise) also maps to noise addition.

Data perturbation is thus the most promising alternative. Clifton and Marks (Clifton & Marks 1996, Clifton 1999) recently indicated new and renewed threats to privacy from mining technology. Clifton's small samples method (Clifton 1999) is not satisfactory as the data is too small to make useful inferences, and individuals whose data is in the sample have no protection. Estivill-Castro and Brankovic (Brankovic & Estivill-Castro 1999, Estivill-Castro & Brankovic 1999) indicated the potential of data perturbation methods and their approach has recently been followed by Agrawal & Srikant (2000).

4.1.2 Mining Paradigms.

The mining paradigm has a great effect on the potential for compromise. For example, the three mining paradigms examined in (Roddick & Lees 2001) differ in the manner in which the results of the mining process are handled as follows:

1. the results of data mining routines fed directly back to the user;

2. the results of data mining are embedded within a process that interprets the results as being merely hints towards further properly structured investigation into the reasons behind the rules; and

Query restriction (QR)	Noise addition
Query size control (Denning 1982, Michalewicz & Yeo 1988), Cell suppression (Kao 1997), Query set overlap control (Adam & Wortmann 1989, Dobkin et al. 1979), Auditing (Chin & Ozsoyoglu 1982, Chin et al. 1984), Maximum order control (Schlorer 1975), Partitioning (McLeish 1989).	Output perturbation (Adam & Wortmann 1989), Data Perturbation (Tendick & Matloff 1994), Random sample techniques (Denning 1980), Probability Distribution Data Perturbation (PDDP) (Adam & Wortmann 1989, Liew et al. 1985).

Table 1: Techniques for privacy in statistical databases

3. there is a knowledge discovery process that accepts an hypothesis and attempts to refine it through the modification of the hypothesis as a result of data mining.

The latter two techniques are ones in which the results of the complete process (including the subsequent research) need not compromise the privacy of individual data.

4.1.3 Inaccurate Data.

The data quality issue is more difficult to resolve. Inaccurate data are undetected by the individual until he or she experiences some associated repercussion, such as a denial of credit, or the withholding of a payment. In some cases, inaccurate data has resulted in dismissal and loss of employment. It is also usually undetected by the organisation, which lacks the personal knowledge necessary for the exposure of inaccuracies. The adoption of data quality management strategies by the organisation, coupled with the expedient correction of any inaccuracies reported by individuals and intermittent data cleansing may go some way to resolving the dilemma. Other solutions are apparent (for example, data matching) but they may have unsatisfactory implications for privacy protection.

4.1.4 Data Security.

The data security issue can be resolved by the introduction of application control mechanisms to MLS databases. One possibility is the employment of intelligent agent technology. A knowledge base of heuristic rules defining permitted and disallowed applications would need to be constructed. A multi-agent system could then be used to monitor and supervise applications in real time. As each user logs in, an agent would be assigned to regulate their queries and perhaps filter their results. The technical complexities of such a system would be a topic of further research.

4.2 Legal solutions

Legal regulation of applied technology is currently one of the more pressing needs facing policy-makers. But how does one approach the development of what is needed? Legislative reform may not be suitable as it is an unwieldy tool in a rapidly expanding technical environment. Common law change is probably a more appropriate and suitable mechanism of legal regulation as it can be creatively applied to novel situations. The disadvantage of the common law, however, is that there needs to be a number of precedent court cases upon which to build common law principles, and litigation in this age of mediated dispute resolution and *in confidence* settlements is becoming a rare phenomenon. Furthermore, the common law's record on subjects such as the protection of privacy and dealing with the legal implications of applied technologies is not strong. This is a rapidly expanding social and business landscape, and the law is failing to keep pace.

Public awareness of the possibility of legal suits alleging negligence and defamation may possibly have some prophylactic effect upon the potential transgressions of contemporary technology. But the subject of individual rights and freedoms is not currently a major curriculum priority in education circles.

Another weakness of legal regulation is the fact that the jurisdictional boundaries that determine the limits of our legal system were drawn up in ignorance of technological developments that render these boundaries virtually irrelevant, given the international structure of many organisations and the burgeoning international presence of an individual on the Internet. If, for example, an Australian were to conduct a transaction and provide data for a multinational organisation registered in Europe via a web site physically situated in the United States, which legal system governs the transaction and its legal repercussions? This is a legal dilemma not lost on international lawyers, and is one that does not readily admit of a simple solution or result.

4.2.1 Structural solutions

The social impact of emerging technology needs to be better understood. One possibility for exploring such impact is the construction of a three-tiered forum for the assessment of a new technology. The lowest level would be institutional, the middle level would be national and the level with the utmost authority would be international. At each level, researchers would present their work to a group of assessors (sociologists, lay people, policy-makers and colleagues) who would attempt to estimate its cultural impacts, and provide some form of impact rating. Governing bodies could use such a rating to determine appropriate applications for the technology. Those cases that cannot find satisfactory reconciliation within the institutional forum would be referred to the national forum and those cases the national forum cannot reconcile would be referred to the international forum. This assessment of potentiality for social disruption would ideally be conducted concurrently to the technology's research.

In the UK, the problem is being addressed by the

Foundation for Information Policy Research – an independent organisation examining the interaction between information technology and society. Their goal is to ... *identify technical developments with significant social impact, commission research into public policy alternatives and promote public understanding and dialogue between technologists and policy-makers in the UK and Europe.*

The foundation combines information technology researchers and people concerned with social impacts and uses a strong media presence to disseminate its arguments and educate the public.

5 Further investigation

The primary consideration of any future research should be at least maintenance, and preferably enhancement, of ethical flexibility. Solutions reconciling any issues must not only be applicable to the ever-changing technological environment, but also flexible with regard to specific contexts and disputes. In addition, we must be able to identify ethical dilemmas as they arise and derive solutions in a timely, preferably concurrent manner. Many ethical issues overlap and have effects on each other. We need to identify any commonalities and differences that exist and exploit them to derive solutions that enable us to uphold, or extend, our ethical standards.

In terms of practical issues, the equality of access argument (the technological *haves and have-nots* (Baase 1997)) has not been considered in this paper. Indeed, data mining may be one context in which the have-nots hold the advantage. In addition, investigation into the application of multi-agent systems to MLS databases provides an interesting possibility for academic research.

Culturally, sociological investigation of the impact of information technology is becoming increasingly urgent. An important social issue not considered here is that contemporary Luddite philosophy (Baase 1997) in fact disempowers humanity, which is, ironically, its philosophical antithesis.

We exist in an environment of rapid change in which technology has an ever-increasing social relevance. The challenge now is to implement a means of assessing an emerging technology's social impact concurrently to its research, providing us with the capacity to use the tools technology provides wisely and with consideration for our culture and its future.

References

Adam, N. R. & Wortmann, J. C. (1989), 'Security-control methods for statistical databases: A comparative study', *ACM Computing Surveys* **21**(4), 515–556.

Agrawal, R. & Srikant, R. (2000), Privacy-preserving data mining, *in* W. Chen, J. Naughton & P. A. Bernstein, eds, 'ACM SIGMOD Conference on the Management of Data', ACM, Dallas, TX, pp. 439–450.

Agrawal, S. & Haritsa, J. (2005), A framework for high-accuracy privacy-preserving mining, *in* '21st Int. Conf. on Data Engineering (ICDE 2005)', IEEE, pp. 193–204.

Agrawal, S., Krishnan, V. & Haritsa, J. (2004), On addressing efficiency concerns in privacy preserving data mining, *in* Y.-J. Lee, J. Li, K.-Y. Whang & D. Lee, eds, '9th Int. Conf. on Database Systems for Advances Applications, DASFAA 2004', Vol. 2973 of *LNCS*, Springer, Jeju Island, Korea, pp. 113–124.

Anderson, R., Johnson, D., Gotterbam, D. & Perrolle, J. (1993), 'Using the new ACM Code of Ethics in decision making', *CACM* **36**(2), 98–107.

Baase, S. (1997), *A gift of fire: social, legal, and ethical issues in computing*, Prentice-Hall.

Berry, M. & Linoff, G. (1997), *Data Mining Techniques — for Marketing, Sales and Customer Support*, John Wiley & Sons, NY, USA.

Bigus, J. (1996), *Data Mining with Neural Networks: Solving Business Problems from Application Development to Decision Support*, McGraw-Hill, NY.

Boyens, C., Gunther, O. & Teltzrow, M. (2002), Privacy conflicts in CRM services for online shops: A case study, *in* C. Clifton & V. Estivill-Castro, eds, 'Privacy, Security and Data Mining', Vol. 14 of *Conferences in Research and Practice in Information Technology*, ACS, Maebashi City, Japan, p. 27.

Brankovic, L. & Estivill-Castro, V. (1999), Privacy issues in knowledge discovery and data mining, *in* C. Simpson, ed., 'AICEC99 Conference Proceedings', Swinburne University of Technology, Australian Institute of Computer Ethics, Melbourne, Australia, pp. 89–99.

Broder, A. (1999), Data mining, the internet, and privacy, *in* B. Masand & M. Spiliopoulou, eds, 'International Workshop WEBKDD '99; Web usage analysis and user profiling', Springer Verlag LNCS 2000, SanDiego, CA, pp. 56–73.

Cavoukian, A. (1998), 'Data mining: Staking a claim on your privacy, online at `www.ipc.on.ca/web_site.eng/matters/sum_pap/papers/datamine.htm`'.

Cavoukian, A. (2004), 'Tag, you're it: Privacy implications of radio frequency identification (rfid) technology'.

Chen, M.-S., Han, J. & Yu, Phillip, S. (1996), 'Data mining: an overview from database perspective', *IEEE Trans. Knowledge and Data Engineering* **8**(6), 866–883.

Chin, F. Y., Kossowski, P. & Loh, S. C. (1984), 'Efficient inference control for range sum queries', *Theoretical Computer Science* **32**, 77–86.

Chin, F. Y. & Ozsoyoglu, G. (1982), 'Auditing and inference control in statistical databases', *IEEE Trans. Software Engineering* **SE-8**(6), 574–582.

Christensen, C. M. (1997), *The innovator's dilemma: when new technologies cause great firms to fail*, Harvard Business School Press.

Clarke, R. (1997), Privacy and dataveillance, and organisational strategy, *in* 'Region 8 EDPAC'96 Information Systems Audit and Control Assoc. Conf', Perth. Australia.

Clarke, R. (1999), Person-location and person-tracking: Technologies, risks and policy implications, *in* '21st Int. Conf. on Privacy and Personal Data Protection', pp. 131–150.

Clifton, C. (1999), Protecting against data mining through samples, *in* 'Thirteenth Annual IFIP WG 11.3 Working Conference on Database Security', Seatle, WA.

Clifton, C. & Estivill-Castro, V., eds (2002), *Privacy, Security and Data Mining - Proc. IEEE Int. Conf. on Data Mining Workshop on Privacy, Security, and Data Mining*, Vol. 14 of *Conferences in Research and Practice in Information Technology*, ACS, Maebashi City, Japan.

Clifton, C., Kantarcioglu, M., Vaidya, J., Lin, X. & Zhu, M. (2002), 'Tools for privacy preserving data mining', *SigKDD Explorations* **4**(2), 28–34.

Clifton, C. & Marks, D. (1996), Security and privacy implications of data mining, *in* 'SIGMOD Workshop on Data Mining and Knowledge Discovery', ACM, Montreal, Canada.

Culnan, M. J. (1993), '"How did they get my name?": An exploratory investigation of consumer attitudes towards secondary information use', *MIS Quarterly* **17**, 341–361.

Custers, B. (2003), *Effects of Unreliable Group Profiling by Means of Data Mining*, LNCS, 2843 edn, Springer-Verlag GmbH.

Denning, D. (1980), 'Secure statistical databases with random sample queries', *ACM Trans. Database Systems* **5**(3), 291–315.

Denning, D. E. R. (1982), *Cryptography and Data Security*, Addison-Wesley.

Dobkin, D., Jones, A. & Lipton, R. (1979), 'Secure databases: Protection against user influence', *ACM Trans. Database Systems* **4**(1), 97–106.

Elmasri, R. & Navathe, S. (2004), *Fundamentals of database systems*, 4th edn, Addison-Wesley, Redwood City, CA.

Estivill-Castro, V. & Brankovic, L. (1999), Data swapping: Balancing privacy against precision in mining for logic rules, *in* M. Mohania & A. Tjoa, eds, 'Data Warehousing and Knowledge Discovery DaWaK-99', Springer-Verlag LNCS 1676, Florence, Italy, pp. 389–398.

Estivill-Castro, V., Brankovic, L. & Dowe, D. (1999), 'Privacy in data mining', *Privacy - Law and Policy Reporter* **6**(3), 33–35.

Evans, L. (1999), 'Big banker is watching, online at `http://www.bankrate.com/brm/news/bank/19990122.asp`'.

Evfimievski, A., Srikant, R., Agrawal, R. & Gehrke, J. (2002), Privacy preserving mining of association rules, *in* 'Eighth ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining', ACM.

Freitas, A. (2000), 'Understanding the crucial differences between classification and discovery of associaiton rules - a position paper', *SIGKDD Explorations* **2**(1), 65–68.

Fule, P. & Roddick, J. F. (2004), Detecting privacy and ethical sensitivity in data mining results, *in* V. Estivill-Castro, ed., '27th Australasian Computer Science Conference (ACSC2004)', Vol. 27 of *CRPIT*, ACS, Dunedin, New Zealand, pp. 159–166.

Gammack, J. & Goulding, P. (1999), 'Ethical responsibility and management of knowledge', *Australian Computer Journal* **31**(3), 72–77.

Gavison, R. (1984), Privacy and the limits of the law, *in* '(Johnson & Nissenbaum 1995)', pp. 332–351.

Gehrke, J., ed. (2002), *Special Issue on Privacy and Security*, Vol. 4 of *SigKDD Explorations*, ACM.

Gordon, M. & Williams, M. (1997), Spatial data mining for health research, planning and education, *in* C. Waegemann, ed., 'Proc. TEPR-97: Towards an Electronic Patient', Medical Records Institute, Newton, MA, pp. 212–218.

Han, J., Huang, Y., Cercone, N. & Fu., Y. (1996), 'Intelligent query answering by knowledge discovery techniques', *IEEE Trans. Knowledge and Data Engineering* **8**(3), 373–390.

Herring, S. (1994), Gender differences in computer-mediated communication: Bringing familiar baggage to the new frontier, *in* V. Vitanza, ed., 'CyberReader', Allen and Bacon, pp. 144–154.

John, G. (1999), 'Behind-the-scenes data mining', *SIGKDD Explorations* **1**(1), 9–11.

Johnson, D. G. & Nissenbaum, H. (1995), *Computers, ethics and social values*, Prentice-Hall, New Jersey.

Kantarcioglu, M., Jiashun, J. & Clifton, C. (2004), When do data mining results violate privacy?, *in* W. Kim, R. Kohavi, J. Gehrke & W. DuMouchel, eds, '10th ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining, KDD '04', ACM Press, Seattle, WA, pp. 599–604.

Kao, M. Y. (1997), 'Total protection of analytic-invariant information in cross-tabulated tables', *SIAM J. Comput* **26**(1), 231–242.

Khaw, Y.-T. & Lee, H.-Y. (1995), 'Privacy and knowledge discovery', *IEEE Expert* **10**(2), 58.

Klang, M. (2004), 'Spyware - the ethics of covert software', *Ethics and Information Technology* **6**(3), 193–202.

Klösgen, W. (1995), 'KDD: Public and private concerns', *IEEE Expert* **10**(2), 55–57.

Laudon, K. C. (1996), 'Markets and privacy', *CACM* **39**(9), 92–104.

Leinweber, D. (1997), 'Stupid data mining tricks: Over-fitting the S&P 500', *First Quadrant Monograph* .

Liew, C. K., Choi, U. J. & Liew, C. (1985), 'Inference control mechanism for statistical database: Frequency-imposed data distortions', *Journal of the American Society for Information Science* **36**(6), 322–329.

Lin, T., Hinke, T., Marks, D. & Thuraisingham, B. (1996), Security and data mining, *in* 'Database Security IX: Status and prospects. Ninth Int. Conf. on Database Security', Vol. 9, Chapman and Hall, pp. 391–399.

McLeish, M. (1989), 'Further results on the security of partitioned dynamic statistical databases', *ACM Trans. Database Systems* **14**(1), 98–113.

Michalewicz, Z. & Yeo, A. (1988), 'Multiranges and multitrackers in statistical databases', *Fundamenta Informaticae XI* pp. 41–48.

Miller, M. (1991), A model of statistical database compromise incorporating supplementary knowledge, *in* B. Srinivasan & J. Zeleznikow, eds, 'Second Australian Database-Information Systems Conference', World Scientific, Sydney.

Miller, M. & Seberry, J. (1989), 'Relative compromise of statistical databases', *Australian Computer Journal* **21**(2), 56–61.

Mills, T. (1997), 'Multi-level secure database management schemes, online at `http://www.sei.cmu.edu/str/descriptions/mlsdms_body.html`'.

NHMRC/AVCC (1997), 'Joint NHMRC/AVCC statement and guidelines on research practice, online at `www.health.gov.au/nhmrc/research/nhmrcavc.htm`'.

OECD (1980), 'Guidelines governing the protection of privacy and transborder flows of personal data, online at `www.oecd.org/dsti/sti/it/secur/prod/priv-en.htm`'.

O'Leary, D. E. (1991), Knowledge discovery as a threat to database security, *in* G. Piatetsky-Shapiro & W. J. Frawley, eds, 'Knowledge discovery in databases', AAAI Press, pp. 507–516.

Peacock, P. R. (1998), 'Data mining in marketing: Part 2', *Marketing Management* **7**(1), 15–25.

Piatetsky-Shapiro, G. (1995), 'Knowledge discovery in personal data vs privacy: a mini-symposium', *IEEE Expert* **10**(2), 46–47.

Pinkas, B. (2002), 'Cryptographic techniques for privacy-preserving data mining', *SigKDD Explorations* **4**(2), 12–19.

Rachels, J. (1975), 'Why privacy is important', *Philosophy and Public Affairs* **4**(4).

Rainsford, C. & Roddick, J. F. (1999), 'Database issues in knowledge discovery and data mining', *Australian Journal of Information Systems* **6**(2), 101–128.

Rindfleisch, T. C. (1997), 'Privacy, information technology and health care', *CACM* **40**(8), 92–100.

Roddick, J. F., Fule, P. & Graco, W. J. (2003), 'Exploratory medical knowledge discovery : Experiences and issues', *SigKDD Explorations* **5**(1).

Roddick, J. F. & Lees, B. G. (2001), Paradigms for spatial and spatio-temporal data mining, *in* H. Miller & J. Han, eds, 'Geographic Data Mining and Knowledge Discovery', Research Monographs in Geographic Information Systems, Taylor and Francis, London, pp. 33–49.

Samuelson, P. (1993), 'Liability for defective electronic information', *CACM* **36**(1), 21–26.

Sarre, R. (2005), The protection of privacy, *in* '(Sarre & Prenzler 2005)', pp. 161–167.

Sarre, R. & Prenzler, T. (2005), *The Law of Private Security in Australia*, Pyrmont, NSW: Thomson LBC.

Saul, J. M. (2001), Legal policy and security issues in the handling of medical data, *in* K. J. Cios, ed., 'Medical Data Mining and Knowledge Discovery', Vol. 60 of *Studies in Fuzziness and Soft Computing*, Physica-Verlag, New York, pp. 21–40.

Schlorer, J. (1975), 'Identification and retrieval of personal records from a statistical data bank', *Methods Inform. Med.* **14**(1), 7–13.

Schreuders, E. & van Kralingen, R. (1998), Klantenkaarten, chipcards en data-mining; een (juridische) verkenning, *in* R. v. Kralingen, M. Lips & C. Prins, eds, 'De kaarten op tafel; Een verkenning van de juridische en bestuurskundige aspecten van chipcards (in Dutch)', SDU Uitgevers, Den Haag, pp. 99–115.

Shoshani, A. (1997), OLAP and statistical databases: Similarities and differences, *in* 'Proc. 16th ACM SIGACT SIGMOD SIGART Symposium on Principles of Database Systems', Tucson, AZ, pp. 185–196.

Spender, D. (1995), *Nattering on the Net: Women, Power and Cyberspace*, Spinifex Publishing, Melbourne.

Stevens, L. (2001), 'It sharpens data mining's focus, *internet week*, online at `http://www.internetweek.com/indepth01/indepth073101.htm`'.

Tavani, H. T. (1999*a*), 'Informational privacy, data mining, and the internet', *Ethics and Information Technology* **1**, 137–145.

Tavani, H. T. (1999*b*), 'KDD, data mining, and the challenge for normative privacy', *Ethics and Information Technology* **1**, 265–273.

Tavani, H. T. (2004), 'Genomic research and data-mining technology: Implications for personal privacy and informed consent', *Ethics and Information Technology* **6**(1), 15–28.

Tendick, P. & Matloff, N. (1994), 'A modified random perturbation method for database security', *ACM Trans. Database Systems* **19**(1), 47–63.

Thuraisingham, B. (1997), Security issues for data warehousing and data mining, *in* 'Database Security X: Status and prospects. Tenth Int. Conf. on Database Security', Vol. 10, Chapman and Hall, pp. 11–20.

UNHCHR (1966), 'International covenant on civil and political rights, online at `www.unhchr.ch/html/menu3/b/a_ccpr.htm`'.

Van Wel, L. & Royakkers, L. (2004), 'Ethical issues in web data mining', *Ethics and Information Technology* **6**, 129–140.

Vedder, A. (1999), 'KDD: The challenge to individualism', *Ethics and Information Technology* **1**, 275–281.

Wagner, J. (1994), Ethical attitudes of mis personnel, *in* 'Managing Social and Economic Change with Information Technology. Proc. 1994 Int. Conf. of the Information Resources Management Association', Idea Group Publishing, pp. 53–57.

Weizenbaum, J. (1972), 'On the impact of the computer on society', *Science* **176**(12), 609–614.

Wilder, C. & Soat, J. (2001), 'Information week research, infoweek'.

Williams, G. (1999), Evolutionary hot spots data mining — an architecture for exploring interesting discoveries, *in* N. Zhong & L. Zhow, eds, 'Proc. 3rd Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD-99)', Springer-Verlag LNAI 1574, pp. 184–193.

Winograd, T. (1992), Computers, ethics and social responsibility, *in* '(Johnson & Nissenbaum 1995)', pp. 25–39.