An Inter-Disciplinary Perspective on the Information Privacy Issue in a Global Environment

AC Jordaan
Department of Economics, University of Pretoria

Y Jordaan
Department of Marketing and Communication Management, University of Pretoria

ABSTRACT

The world economic system's transformation from a dominantly mass-production model, to a mass-customisation model is seen as creating a demand for personal information on consumers. This has lead many consumers to feel the need to protect their information because businesses request personal information during commercial transactions. This conceptual paper addresses information privacy as a marketing-related issue with an inter-disciplinary nature and aims to illustrate how marketing and economics can work together in a more cohesive manner. The information privacy issue is presented as striking a fair balance between the privacy interests of consumers, the financial interests of businesses, and the sustainability of an economy in the global environment. The paper concludes that consumer information privacy will always remain an issue of protection for consumers, an ethical issue for marketers, and is fast becoming an issue of social responsibility for government.

JEL A12, 13, D82

INTRODUCTION

Consumer privacy issues are not new and the right to privacy is guaranteed through many official documents on human rights of various countries. However, there is growing consumer concern about personal information used by government and private commercial businesses (Turner & Varghese, 2002: 11). The Internet has contributed, particularly with respect to its use as a tool for communication, entertainment, and marketplace exchange (Miyazaki & Fernandez, 2001: 28). The consumer privacy issue is taking on greater magnitude as an increasing number of consumers are involved in marketing transactions, and progressively more marketers rely on technology in their day-

to-day operations. Businesses rely on the consumer information they gather in daily transactions to participate in an ever-increasingly competitive economic environment. This is in line with the theory of a market economy which is based on profit maximisation, where acquiring consumer information is vital in competing and ensuring a profitable return.

In this paper, using an inter-disciplinary approach, some effort is made to address consumer information privacy from a marketing, economic, and global perspective, with reference to South Africa as one of the role players in the global environment. The purpose of the paper is to describe how consumers' perceived threat of the loss of personal privacy and of globalisation forces countries to create national policies that are harmonised with international policy frameworks. This moves the information privacy issue beyond the scope of marketing, turning it into an issue of social responsibility for government and industry.

THE INFORMATION PRIVACY ISSUE

The right to privacy has become widely recognised all over the world. It is expressly guaranteed in the Universal Declaration of Human Rights of 1948, the European Convention on Human Rights of 1950, the International Covenant on Civil and Political Rights of 1966, and the American Convention on Human Rights of 1969. It is not explicitly mentioned in the African Charter on Human and Peoples Rights of 1981, but is found in most domestic bills of rights, for example the Bill of Rights in the South African Constitution of 1996 (Devenish, 1999: 135).

One of the first definitions of privacy was documented by Warren and Brandeis (1890: 193) in the 1800s. They reasoned that the right to life refers to the right to enjoy life, resulting in the right to be let alone. One constant across the history of privacy is the difficulty of defining the concept of privacy. Privacy is an elusive, value-laden concept, and it is hard to reach consensus on a universally accepted definition, since this concept means different things to different people at different times (Gellman, 2002). Academic literature includes contributions from many different disciplines addressing the meaning of privacy. Although the purpose of this paper is not to solve the definitional problem of privacy, several definitions are provided to serve as a background for the discussion.

In Europe, the right to privacy has been defined to consist in "essentially the right to live one's own life with a minimum of interference" (Devenish, 1999: 137). In Australia, privacy is defined as "people's right to the privacy of their own body, private space, privacy of communications, information privacy, and

freedom from surveillance" (Collier, 1995: 44). The Royal Bank of Canada defines information privacy as "the right of customers to have their personal information safeguarded and to determine for themselves how, and to what extent, information about them is collected, used and communicated to others" (Jayson, 2002: 3).

Westin (in Agre & Rotenberg, 1998: 194) contends that no durable definition of privacy is possible because privacy issues are fundamentally matters of values, interests, and power. Privacy itself is an intangible commodity and is often categorised in a negative sense. For example, privacy is 'invaded', a confidence is 'breached', or a trust is 'broken' (Pounder & Kosten, 1992: 1). Violations of privacy can constitute an invasion of a person's private life or relate to the acquisition and disclosure of personal information. The invasion of privacy has been defined as "an international and wrongful interference with another's right to seclusion in his or her private life" (Devenish, 1999: 145).

Privacy, but specifically information privacy, is currently on the public agenda of many countries (Holvast, Madsen & Roth, 2001: 14). This paper will focus on consumer privacy, where information privacy is defined as the right of consumers to safeguard information about themselves from the use or control by businesses. Many consumers feel the need to protect their information because businesses request personal information during daily commercial transactions. The next section will discuss the concept of information exchange between consumers and businesses.

INFORMATION EXHANGE

Every exchange requires two or more parties where one party offers something and another party obtains that which is given by offering something in return (Kotler, 2000: 12). Consumers invest, besides money and other costs, their personal information in an exchange process. Exchange may be viewed either from the perspective of economic exchange or of social exchange. In economic exchange models, social interaction is viewed as an exchange of mutually rewarding activities in which the receipt of a needed valuable is contingent on the supply of a favour in return. According to social exchange theory, social relationships are based on each partner's motivational investment and anticipated social gain (Takala & Uusitalo, 1996: 47). Whatever the reward, it has been suggested that transactions are more likely to be morally defensible if both parties enter them freely and fully informed (Kavali, Tzokas & Saren, 1999: 578). Exchange is a value-creating process because it normally leaves both parties better off. This results in a code of conduct to which both parties should subscribe and is described by social contracts.

A social contract is "that fundamental compact that consists of the rules imposing basic duties, assigning rights, and distributing the benefits of political, social, and economic cooperation, unanimously agreed to by reasonable people in a state of perfect equality and absolute impartiality" (Grant, 2000: 19). In a marketing context, a social contract occurs when a customer provides a marketer with personal information at the point of purchase with the intention that the marketer will use this information to serve the customer better (Milne, 1997: 299). The belief that information control is a key mediator of consumer privacy concerns has led many to suggest that marketers should view consumers' exchange of personal information as an implied social contract (Culnan 1995: 11; Milne, 1997: 299). When marketing is viewed as an implied social contract, consumers provide personal information in exchange for products or services, receiving solicitations and other information, based on an expectation that their personal information will be managed responsibly. According to Phelps, Nowak & Ferrell (2000: 29) the implied social contract is considered breached if consumers are unaware of information being collected, if the marketer discloses the consumer's personal information to a third party without permission, or if consumers are not given an opportunity to remove their names from lists or otherwise restrict the dissemination of their personal information.

As the extensive use of consumer information has become part of the fabric of the modern marketplace, the issue of who owns the consumer's information is raised (Davis, 1997: 35). The control of consumer information has proved a valuable commodity in the marketplace and is therefore a source of power (Prabhaker, 2000: 164). Information technology is having a major impact in this area by changing the nature of relationships and the balance of power between the parties involved (Fletcher & Peters, 1996: 147). In practice, consumers and businesses often disagree about who owns the data and what kinds of trade-off are acceptable in different situations (Campbell, 1997: 47). Several perspectives on ownership have been offered, placing ownership rights either in the hands of consumers or in those of business.

One view suggests that businesses that have gathered consumer information through the expenditure of time, effort, and money should be able to control the use and dissemination of the information (Davis, 1997: 35). This is supported by Taylor, Vassar and Vaught (1995: 44) who suggest that marketers who have created databases own the information contained in these databases and can therefore use, sell or rent this information to others without consumers' consent. Another view suggests that if personal information can be defined as a property, the original owner should control its use and dissemination. This idea is consistent with those of Westin and Miller (in Davis, 1997: 35) who argued in the late 1960s that property rights should be attached to personal information so that individuals are better able to control its dissemination and safeguard their

personal privacy. Foxman and Kilcoyne (in Davis, 1997: 34) argue, on ethical grounds, that marketers should recognise consumer ownership rights to personal information, in that consumers perceive these rights to exist and resent their violation. Some believe that placing ownership in the hands of consumers could improve consumer targeting and solicitation response rates. This is because consumers who grant permission for contact may be better qualified prospects and more interested in future exchange transactions (Davis 1997: 39).

It is important to realise that there can be no transaction or exchange without the communication of information (Yudelson, 1999: 63). The world economic system's transformation from a dominantly mass-production model to a mass-customisation model is seen as creating an enormous demand for detailed data on the behaviour of consumers (Agre & Rotenberg, 1998: 277). At this point, an inter-disciplinary framework for information exchange will be used to explain the dual nature of the information privacy issue. On the one hand, it is concerned with the information exchange between consumers, who have a right to privacy, and businesses, that have a right to a free flow of information. (This will be discussed in the next section from a marketing perspective representing the micro level effects of information privacy). On the other hand, it is concerned with the participation of these role players in a national economy. If market imperfections, such as the lack of information privacy, occur in the market, and industry cannot regulate itself successfully, government may be forced to intervene in terms of data protection actions. (This will be addressed from an economic perspective representing the macro level effects of information privacy). The remainder of the paper will be presented as striking a fair balance between the information privacy interests of consumers, the financial interests of businesses, and the sustainability of an economy in the global environment.

MICRO LEVEL EFFECTS OF INFORMATION PRIVACY

Yudelson (1999: 63) conceptualised marketing as "those activities who seek to influence voluntary exchange transactions in a wide range of settings and situations where both parties may look beyond the specific exchange transaction to the development of a mutually beneficial relationship during an extended period of time". As the relationship between two parties develops over time, consumer-business relationships may well develop along more tightly defined lines, even if this involves introducing more contractual elements into the interaction (Peters, 1997: 221). To understand the relationship between the parties involved, one has to understand the objectives and expectations of each party. Businesses strive for continuing relationships because it is assumed that these relationships are more profitable (Takala & Uusitalo, 1996: 48). Consumers' expectations, in turn, extend beyond the provision of the actual

good or service to the manner in which their information is obtained, stored, and used by businesses (Campbell, 1997: 47). Let us take a closer look at the effect of information privacy on each party in an exchange relationship.

Consumers have little or no control over the prospecting efforts of businesses. The sheer volume of direct mail, phone calls and e-mails relates to the physical intrusion of marketing communications into the daily lives of consumers (Katzenstein & Sachs, 1992: 71; O'Malley, Patterson & Evans, 1999: 442). If consumers could control the extent of marketing solicitations, it would offer advantages as well as disadvantages from a social and economic perspective. One advantage would be the protection that personal information privacy rights provide against unwanted mail and telephone solicitations (Davis, 1997: 39). A social disadvantage to information privacy is the situation where consumers cut themselves off from valuable marketing information by failing to provide consent to information use and dissemination (Davis, 1997: 39).

Much of recent attention to privacy issues has focused on the Internet. Consumers experience a perceived threat to their individual privacy owing to the staggering and increasing power of information-processing technology to collect a vast amount of information about them. This information is often stored, analysed, interpreted, compared and exchanged by businesses on the Internet, often without the knowledge or control of consumers. While businesses may claim that they apply tight security and confidentiality controls over the information, these controls are often for the benefit of the business and may provide little protection to consumers (Collier, 1995: 41).

Many consumers will not purchase items on the Internet if they fear that their personal information will be misused. Some spend time and money solely to evade the consequences of too much information sharing (Gellman, 2002). The costs incurred by consumers to protect themselves from unwanted view or intrusion constitute a privacy toll paid in both money and time. The privacy toll includes costs associated with higher prices, stopping junk mail and telemarketing calls, and protecting privacy on the Internet (Gellman, 2002). As consumers become more comfortable online, they are increasingly open to providing personal information to their favourite websites. But they are stridently demanding that this information be used to enhance their experience and that the information must not be used in ways that abuse a privileged relationship, or even be subject to a perception of abuse. Online businesses face a delicate balance between strong consumer demand for privacy protection and a real consumer desire for personalised treatment (Mabley, 1999: 1).

Businesses have good reason to collect information about customers. It enables them to target their most valuable prospects more effectively, tailor their

offerings to individual needs, improve customer satisfaction and retention, and identify opportunities for new products or services. A generally accepted assumption in any market-oriented economy is that businesses will aim to maximise their profits (Mabley, 1999: 4). The profit maximisation principle can have an affect on consumers in that it tends to point towards the selfish motives of businesses. It is important to realise that the forces of competition in the market environment prevent many businesses from being too generous in respect of consumer information privacy protection. Sometimes the consequences of pursuing profit maximisation have a detrimental effect on consumers to the extent that it becomes socially undesirable. Social responsibility is defined as "doing business in a way that maintains or improves both the customer's and society's well-being" (Mohr, Webb & Harris, 2001: 46). Most definitions of social responsibility emphasise that a socially responsible business must have concerns beyond short-term profitability. The question here is whether, and in what circumstances, businesses will be willing to forgo profits or other benefits to themselves in order to avoid harm to consumers.

It follows that customer relationships lie at the core of marketing and should be developed so that consumer and business objectives are met (Grönroos, 1990: 5). While these objectives may or may not in fact be independent, the means of satisfying them are very often interdependent on each other, as well as being dependent on the economic system (Peters, 1997: 223). This highlights the importance of the economic environment within which consumer-business relationships are developed. This will be discussed in the next section.

MACRO LEVEL EFFECTS OF INFORMATION PRIVACY

The lack of information privacy experienced by consumers and businesses is an indication that a universal market imperfection is currently evident in many economies. From an economic perspective, this imperfection in the market places the economy in disequilibrium, and one needs to determine the conditions or relationships that have to be satisfied to reach a condition of equilibrium again.

In economic models, equilibrium conditions arise from the maximising behaviour of businesses and consumers. Suppose an economy operates under perfectly competitive conditions with no market imperfections, no negative externalities in production or consumption, and no public goods. In such a situation, perfect information exists, all resources are privately owned, businesses maximise profit, and consumers maximise utility. Finally, markets always clear and there are no adjustment costs or unemployment of resources. In

this type of economy, the optimal government policy is a laissez-faire approach, and the resulting equilibrium is referred to as a first-best condition. This kind of market condition can be seen as economic *paradise* since there is no conceivable way of increasing economic efficiency any further (Suranovic, 1999). However, real-world economics is unlikely to be so perfect, since market imperfections are part of any economy.

As soon as a market imperfection, such as the lack of information privacy, is introduced into an economic *paradise* environment, the resulting equilibrium is less than optimum, reducing the optimal level of national welfare. This situation is called a second-best equilibrium and is known as 'the theory of the second-best'. Formulated by Richard Lipsey and Kelvin Lancaster (1956), the second-best equilibria arise whenever all the equilibrium conditions satisfying economic *paradise* cannot occur simultaneously. The principles of this theory have important implications for the understanding of potential interventions in situations of market imperfection.

In this paper, it is assumed that the lack of consumer information privacy is a market imperfection and therefore implies that the economy starts at a second-best equilibrium. The theory of the second-best posits that when markets have imperfections, it is possible to add another carefully designed 'imperfection' (such as a privacy policy) to improve economic efficiency. The reason for this outcome is that the second imperfection (a privacy policy) could correct the inefficiencies of the first imperfection (lack of information privacy) by more than the inefficiencies caused by the second imperfection (Suranovic, 1999). In other words, interventions that would reduce national welfare in the absence of imperfections can now improve welfare when there are imperfections present. Even though the intervention may not correct the imperfections completely, it may reduce the detrimental effects of the imperfection, and a new and better equilibrium position will be obtained. A general rule to identify first-best equilibrium is to use an intervention method that most directly addresses the market imperfection.

Self-regulation by industry is one approach available to address market imperfections and is mainly represented by ethical codes. Ethics are the moral principles and values that govern the way consumers and businesses conduct their activities (Churchill & Peter, 1998: 129). To become and remain part of the economic environment, ethical codes have to be accepted by all parties. There will thus be a need for businesses to make the codes explicit, to iterate their doctrine and to make their presence felt. It is clearly in the interest of those who are obeying the codes to enforce them, to call attentions to violations and to use the ethical and social pressures of the society at large. Unfortunately, self-regulation has its limitations. First, most consumer groups lodge complaints to

government agencies instead of to the industry. Second, interests of businesses are diverse and one industry solution is hardly possible. Third, not all businesses are members of a national controlling body, especially those most apt to act in unethical ways. Finally, industry boards have no power to enforce compliance (Katzenstein & Sachs, 1992: 73).

The above-mentioned limitations may lead to a situation where the market cannot correct itself in terms of self-regulation. This can be seen as a market imperfection and warrants government intervention. Government should use the most efficient (least costly) method to reduce inefficiencies caused by imperfections. If government were to add information privacy legislation, for example, this would reduce the negative aggregate effects caused by the lack of information privacy and thus raise national welfare. When government intervention corrects the imperfections completely, the economy would revert to economic *paradise* (Rebello, 2002: 14).

From the above discussion it is clear that the lack of information privacy is a market imperfection causing the economy to operate at a second-best equilibrium condition. The globalisation of markets has also forced countries to address the market imperfections and to adopt privacy legislation. This can have an effect both on businesses in a market-driven economy, in terms of their principle of profit maximisation, and on a country's economic growth, in terms of its trading with other countries. The final section of this paper will address information privacy in a global environment. In this section, the focus will also be on South Africa as one of the role players in the global environment, and its current position on the information privacy issue with regard to data protection legislation.

INFORMATION PRIVACY IN A GLOBAL ENVIRONMENT

The reason for government intervention in an economy was explained earlier as a reaction to market imperfections. Government can intervene on the basis of the fact that the market is unable to resolve the information privacy problem by means of self-regulation. As the global marketplace continues to expand, businesses face increasingly strict privacy and data protection regulations in a growing number of countries around the world. It is therefore important for countries to take cognisance of the international privacy regulatory environment. A brief overview of the main historical developments with regard to privacy and data protection in the international arena follows.

In 1969 the Organisation for Economic Cooperation and Development (OECD), an international body of 29 countries, became the first international organisation

to recognise the privacy implications of trans-border data flows of personal information (Holvast, Madsen & Roth, 2001: 1). The Privacy Protection Act was passed in the United States in 1980 (Rotenberg, 2001: 101). In the same year, the OECD issued guidelines for privacy protection in the transfer of personal information across national borders. (Rotenberg, 2001: 268). Canada passed their Privacy Act in 1982 (Holvast, Madsen & Roth, 2001: 2). The United Kingdom's Data Protection Act was put in place in 1984, stopping personal information from international transfer if it was considered such information was not adequately protected in the receiving country (Collier, 1995: 42). In 1985, the OECD extended their guidelines to cover trans-border data flow, and the Council of Europe concluded the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Rotenberg, 2001: 297). In Australia, the Privacy Act of 1988 details Information Privacy Principles based on the OECD Guidelines (Rotenberg, 2001: 413).

In 1995, the European Union's Directive on the Protection of Personal Data and on the Free Movement of Such Data finally emerged from the European Union's complex and drawn-out legislative process (Agre & Rotenberg, 1998: 105). The Data Protection Directive has had, and will continue to have, an impact on the data-protection policies of countries (or states) that have not yet passed such legislation, including those outside the European Union. The pressure on non-European Union countries stems principally from the stipulation in Article 25 that data transfers to a 'third country' may take place only if that country ensures an 'adequate level of protection' (Agre & Rotenberg, 1998: 109). The Australian Parliament passed the Privacy Amendment (Private Sector) Bill in December 2000. The new legislation contains amendments to the Commonwealth Privacy Act of 1988 and will regulate the handling of personal information by private sector organisations (Rotenberg, 2001: 413).

On 21 July 2000, the United States Department of Commerce, responding to possible restrictions of personal data from Europe to the United States as a result of the European Union Data Privacy Directive, issued what is known as its 'Safe Harbor Privacy Principles'. The Safe Harbor programme was agreed to after the United States insisted that a voluntary approach to data privacy was better than a legislative approach (BNA, 2002: 191). United States organisations acceding to the 'safe harbor' principles are seen by the United States as fulfilling the adequate protection requirement of the European Union Directive (Holvast, Madsen & Roth, 2001: 14). The Personal Information Protection and Electronic Documents Act of 2000 came into force in Canada on 1 January 2001. This Act establishes rules that govern the collection, use and disclosure of personal information in the private sector (Kirwin, 2002). The latest international development that took effect on 31 July 2002 was the new European Union Directive on the protection of personal data and privacy in the electronic

communications sector. This new Directive introduces new rules on data retention and unsolicited commercial communications (Mason, 2002).

Given the above, it is evident that protection of personal data transfers varies from nation to nation, as does the regulatory framework governing them. There is also a marked shift in the direction of a global standard for information privacy modelled on the provisions of the European Union (Rudraswamy & Vance, 2001: 133). It is clear that the European Union's 1995 Data Protection Directive constitutes the rules for the increasingly global character of data-processing operations. Increasing global interdependence has possible consequences for those businesses that rely on the unimpeded flow of personal information and that cannot claim to protect the data of consumers in ways that match the European standard (Agre & Rotenberg, 1998: 111). In an interdependent world, the policy efforts of the Europeans carry externalities that force other countries to pursue policies that they would otherwise oppose or avoid. In addition, the general pressures to conform have increased as more and more countries have joined the 'data-protection club'.

South Africa is currently lagging behind in terms of data protection despite the following legislative actions that have been taken. In the Bill of Rights, Chapter 2 of the South African Constitution, South African citizens are guaranteed (among other things) the right to privacy and the right to access of information. The Promotion of Access to Information Act 2 of 2000 was promulgated to give effect to the constitutional right of access to any information held by the state, as well as any information that is held by another person and that is required for the exercise or protection of any rights. However, this Act excluded private section portions and data protection provisions. This led to a request by the Minister to form a Committee (Project 124) to investigate the privacy and data protection issue with the aim of improving existing legislation and adding new legislation in the future.

The Electronic Communications and Transactions (ECT) Bill was tabled before Parliament recently and South Africa became the first country in Africa to join more than 20 countries that have introduced electronic commerce legislation in the past four years (Temkin, 2002: 2). Using a smart card, a fingerprint and a password, President Thabo Mbeki signed into law the Electronic Communications and Transactions (ECT) Bill in July 2002. The ECT Act makes advanced electronic signatures legal, easing the conclusion of deals and transactions online. Despite the advantages of electronic communications and transactions, it also poses renewed threats to information privacy. The most controversial part of the act is Chapter 10, which allows for a non-profit organisation to control the '.za domain' (Anon, 2002: 2). This organisation's nine directors will be nominated by the minister, demonstrating a high level of

regulation by the South African government. Considering the South African government's lack of proper data protection legislation compared to the rest of the world, this Act demonstrates excessive control in an area that is not regulated by any other country.

South Africa has to realise that adequate privacy protection is becoming a necessary condition for being on the global information highway. A lack of proper regulatory frameworks may have far-reaching social and ethical implications, particularly when countries fail to comply with existing global regulations (Rudraswamy & Vance, 2001: 133). Whatever privacy laws the international community adopt, there will be strong and irresistible pressure for South Africa to follow suit.

CONCLUSION

Information privacy is not an issue that will be resolved quickly, and it may require a multi-faceted approach involving a combination of self-regulation efforts, privacy policies and legislation. It is therefore vital for consumers, businesses and government to accept the challenge and commit themselves to an enhanced economic environment. All parties will be worse off if the urgency of the matter is not accepted and addressed. Countries that neglect to address information privacy concerns will increasingly be confronted to comply with international accepted privacy codes and standards. This is a situation that a country can ill afford within the current competitive global economy.

Important to all market participants are the inherent transaction factor of mutual gain and the general acceptance of ethical obligations to become and remain part of the economic environment. Information privacy is no longer only a consumer-related issue that needs to be addressed by marketers on a micro level; it has become an issue of national concern that needs to be addressed by government on a macro level. Consumer information privacy will remain an issue of protection for consumers and an ethical issue for businesses, and it is fast becoming an issue of social responsibility for government. Globalisation is forcing countries to implement relevant privacy legislation to ensure continued participation and sustainable economic growth.

REFERENCES

1 AGRE, P.E. & ROTENBERG, M. (1998) *Technology and Privacy: The New Landscape*, (1st ed.) Cambridge: MIT Press.

2 ANON (2002) "Internet-related bill becomes law", *City Press*, 4 August: 2.
3 BUREAU OF NATIONAL AFFAIRS (2002) "EU says transparency, enforcement problems need attention in US Safe Harbor program", *Privacy & Security Law*, 1(8): 191.
4 CAMPBELL, A.J. (1997) "Relationship marketing in consumer markets: a comparison of managerial and consumer attitudes about information privacy", *Journal of Direct Marketing*, 11(3): 44-57.
5 CHURCHILL, G.A. & PETER, J.P. (1998) *Marketing: Creating Value for Customers* (2nd ed.) Boston, Massachusetts: Irwin McGraw-Hill.
6 COLLIER, G. (1995) "Information privacy", *Information Management & Computer Security*, 3(1): 41-45.
7 CULNAN, M.J. (1995) "Consumer awareness of name removal procedures: implications for direct marketing", *Journal of Direct Marketing*, 9(2): 10-19.
8 DAVIS, J.F. (1997) "Property rights to consumer information", *Journal of Direct Marketing*, 11(3): 32-43.
9 DEVENISH, G.E. (1999) *A Commentary on the South African Bill of Rights*. Durban: Butterworth Publishers (Pty) Ltd.
10 FLETCHER, K. & PETERS, L. (1996) "Issues in customer information management", *Journal of the Market Research Society*, 38(2): 145-60.
11 GELLMAN, R. (2002) "Privacy, consumers, and costs: how the lack of privacy costs consumers and why business studies of privacy costs are biased and incomplete", *Electronic Privacy Information Center*, Research report available online at http://www.epic.org/reports/dmfprivacy.htm.
12 GRANT, R. (2000) "The social contract and human rights", *The Humanist*, Jan/Feb: 18-23.
13 GRöNRNROOS, C. (1990) "Marketing redefined", *Management Decision*, 28(8): 5-9.
14 HOLVAST, J., MADSEN, W. & ROTH, P. (2001) *The Global Encyclopedia of Data Protection Regulation*, Supplement No. 3. Netherlands, The Hague: Kluwer Law International.
15 JAYSON, S. (2002) "Privacy: a matter of trust", *Privacy Daily*, 14 May: 1-9, available online at http://privacydaily.privacycouncil.com.
16 KATZENSTEIN, H. & SACHS, W.S. (1992) *Direct Marketing*, (2nd ed.) New York, USA: MacMillan Publishing Company.
17 KAVALI, S.G., TZOKAS, N.X. & SAREN, M.J. (1999) "Relationship marketing as an ethical approach: philosophical and managerial considerations", *Management Decision*, 37(7): 573-81.
18 KIRWIN, J. (2002) "EC endorses Canadian data privacy as adequate to handle Europeans' data", *Privacy Law Watch*, 15 January, available online at http://pubs.bna.com.

19 KOTLER, P. (2000) *Marketing Management*, The Millennium Edition. New Jersey, USA: Prentice-Hall.
20 LIPSEY, R.G. & LANCASTER, K. (1956) "The general theory of the second-best", *Review of Economic Studies*, 24:11-32.
21 MABLEY, K. (1999) "Privacy vs personalisation: a delicate balance", *Cyber Dialogue*, available online at http://www.cyberdialogue.com.
22 MASON, M. (2002) "EU publishes directive on data protection in electronic communications", *PX NewsFlash*, 9 August, available online at http://www.privacyexchange.org/news/index.html.
23 MILNE, G.R. (1997) "Consumer participation in mailing lists: a field experiment", *Journal of Public Policy and Marketing*, 16(2): 298-310.
24 MIYAZAKI, A.D. & FERNANDEZ, A. (2001) "Consumer perceptions of privacy and security risks for online shopping", *Journal of Consumer Affairs*, 35(1): 27-44.
25 MOHR, L.A., WEBB, D.J. & HARRIS, K.E. (2001) "Do consumers expect companies to be socially responsible? The impact of corporate social responsibility on buying behaviour", *Journal of Consumer Affairs*, 35(1): 45-61.
26 O'MALLEY, L., PATTERSON, M. & EVANS, M. (1999) *Exploring direct marketing*, London: International Thomson Business Press.
27 PETERS, L.D. (1997) "IT enabled marketing: a framework for value creation in customer relationships", *Journal of Marketing Practice: Applied Marketing Science*, 3(4): 213-29.
28 PHELPS, J., NOWAK, G. & FERRELL, E. (2000) "Privacy concerns and consumer willingness to provide personal information", *Journal of Public Policy and Marketing*, 19(1): 27-42.
29 POUNDER, C. & KOSTEN, F. (1992) *Managing data protection*, (2nd ed.) London: Butterworth-Heinemann Ltd.
30 PRABHAKER, P.R. (2000) "Who owns the online consumer?" *Journal of Consumer Marketing*, 17(2): 158-71.
31 REBELLO, J. (2002) *The problem of second-best: Are partial equilibrium and third-best analyses solutions?* Paper delivered at the Advanced Antitrust. http://home.uchicago.edu/
32 ROTENBERG, M. (2001) *The Privacy Law Sourcebook 2001: United States Law, International Law, and recent developments*, (1st ed.) Washington, DC: EPIC Publications.
33 RUDRASWAMY, V. & VANCE, D.A. (2001) "Transborder data flows: adoption and diffusion of protective legislation in the global electronic commerce environment", *Logistics Information Management*, 14(1/2): 127-36.
34 SURANOVIC, S. (1999) *The theory of the second best*. http://internationalecon.com

35 TAKALA, T. & UUSITALO, O. (1996) "An alternative view of relationship marketing: a framework for ethical analysis", *European Journal of Marketing*, 30(2): 45-60.

36 TAYLOR, R.E., VASSAR, J.A. & VAUGHT, B.C. (1995) "The beliefs of marketing professionals regarding consumer privacy", *Journal of Direct Marketing*, 9(4): 38-46.

37 TEMKIN, S. (2002) "Experts say bill offers exciting opportunities", *Business Day*, 5 March: 2.

38 TURNER, M.A. & VARGHESE, R. (2002) "Making sense of the privacy debate: a comparative analysis of leading consumer privacy surveys", *Privacy & American Business*, The American consumer and privacy: P&AB's annual round-up and analysis of privacy surveys, as discussed at the 8th Annual National Conference "Managing the new privacy revolution", 20-22 March, Washington, DC.

39 WARREN, S.D. AND BRANDEIS, L.D. (1890) "The right to privacy", *Harvard Law Review*, IV(5): 193-220.

40 YUDELSON, J. (1999) "Adapting to McCarthy's four P's for the twenty-first century", *Journal of Marketing Education*, 21(1): 60-7.