Y Jordaan
AC Jordaan

Communicating the protection of information privacy

ABSTRACT

The world economic system's transformation from a dominant mass-production model to a mass-customisation model is seen to have created a demand for personal information from consumers. This has led to many consumers feeling the need to protect their information as businesses request increasingly more personal information during commercial transactions. This conceptual paper addresses information privacy as an inter-disciplinary issue that affects relationships at micro, macro and global levels. First at micro level, addressing the value perception of information among consumers and marketers; secondly at macro level, illustrating the role of the government in protecting information privacy; and thirdly at global level, since the flow of information plays a major role in eliminating boundaries between countries. Finally, the managerial implications of information privacy are discussed, concluding that effective customer relations now require businesses to communicate in ways that make their customers feel protected.

Dr. Yolanda Jordaan is a Senior Lecturer in the Department of Marketing and Communication Management, University of Pretoria. Prof André Cillié Jordaan is an Associate Professor in the Department of Economics at the same University.

1. INTRODUCTION

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 Brande (1890:193) in the 1800s. They reasoned that the right to life refers to the right to enjoy life, and the right to be left alone. One constant across the history of privacy is the difficulty of defining the concept of privacy. Westin (1995:194) 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 may constitute an invasion of a person's private life or relate to the acquisition and disclosure of personal information (Devenish, 1999:145).

This paper focuses 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. Information privacy will be addressed on different levels, using an inter-disciplinary approach: first at micro level, where the value perception of information among consumers and marketers is discussed; secondly at macro level, illustrating the role of the government in the information privacy issue; and finally at global level, since the flow of information plays a major role in eliminating boundaries between countries.

2. INFORMATION PRIVACY AT MICRO LEVEL

The evolution of marketing and the advocacy to extend marketing into the management of the relational exchange processes within consumer markets have meant a growing interest in treating customers on an individual basis. The search for improved techniques in obtaining and retaining customers, and the increasing availability, sophistication and cost-effectiveness of computer-based systems have been paralleled by an increasing concern among consumers about the impact of these new marketing management techniques on their private rights (Long, Hogg, Hartley & Angold, 1999:5).

Underlying any definition of information privacy is an implicit understanding that consumers' interests are balanced against those of society at large. Consumers surrender a measure of privacy in exchange for some economic or social benefit (Culnan, 1993:341). It is important to realise that there can be no transaction or exchange without the communication of information. The information need not be complete or even accurate but, as a minimum, the two parties must know about each other's existence. They must have some ideal of what will be exchanged and what the respective benefits and costs may be (Yudelson, 1999:63). To develop a marketing relationship, consumers must perceive that the benefits derived from the relationship with the marketer outweigh the costs (Davis, 1997:33).

At this point, the dual nature of the information privacy issue should be stressed. On the one hand, it is concerned with consumers' right to privacy. On the other hand, information protection negatively affects businesses in their right to full disclosure and free flow of information (Walczuch & Steeghs, 2001:142). The tension between information access and information control has been presented as a problem of striking a fair balance between the privacy interests of consumers and the financial interests of businesses (Campbell, 1997:47).

Information has increasingly emerged as an asset with a market value and associated acquisition and handling costs. As an asset, information can have the property of increasing in value through use (Glazer, 1991:6). Therefore, the focus for customers is likely to be on the value they receive from the demonstrated use of their information by businesses. By contrast, it is likely that for the marketer, customer information value may be sought from the anticipated use of such information (Peters, 1997:218). However, where customers do not see the collection of customer data as resulting in greater value, discrepancies may arise. This distinction between anticipated and realised information value on the part of businesses can lead to problems of goal incompatibility with customers and may well raise issues of privacy. This may create a perception among customers that businesses do not really need, or appropriately use, the information they collect from customers (Peters, 1997:219).

Many businesses find customer profile information to be an important ingredient for relationship building. It provides an advantage in a competitive marketplace where knowledge about the target buyer needs to be more detailed, more personal, and increasingly timely (Franzak, Pitta & Fritsche, 2001:634). However, the current data avarice, which leads marketers to seek out and capture more personal information, has a definite downside. The more effective the information gathering, storage and retrieval process becomes, the greater the tendency will be to encroach on individual privacy (Fletcher & Peters, 1996:148).

One of the most profound implications of information-processing technology is the realisation that traditional trade-offs may be obsolete. This can be illustrated by the withdrawal of a customer database by EasyInfo. In early 2002, EasyInfo.co.za (South Africa's first online telephone directory) launched a directory of 2.5 million names and addresses. Soon afterwards, EasyInfo, newspapers and radio stations were bombarded with complaints from consumers about an invasion of privacy and only weeks later, EasyInfo had to close its information site (Marud, 2002:1; Venter, 2002:3). This example highlights the importance of marketers addressing consumers' needs, wants and concerns pertaining to the collection, use and dissemination of their personal information. The marketing industry, specifically the direct marketing industry, has taken steps to address some of the major information privacy concerns. Below follows a brief discussion on industry self-regulation as a means of addressing consumer privacy concerns in an attempt to restore and maintain marketing relationships.

2.1 The role of self-regulation in information privacy

Information privacy issues, for both business and customers, may be alleviated by the marketing industry's increased attempts to police itself (O'Malley, Patterson & Evans, 1999:441). Direct Marketing Associations worldwide have set privacy guidelines as an important step in creating meaningful self-regulation to protect consumer privacy in the information age. These associations provide privacy policy guidelines to their member organisations in an effort to build consumer trust. Private sector leadership is critical in building consumer confidence in the marketplace by ensuring that personal information will be treated fairly and responsibly (Anon., 1999:6).

Unfortunately, self-regulation has its limitations. Firstly, the success of self-regulation is dependent upon consumers using the facilities provided by the industry, such as registering the complaints of offending businesses. Secondly, most consumer groups lodge complaints with government agencies instead of with industry. Thirdly, the interests of businesses are diverse and one industry solution is hardly possible. Fourthly, not all businesses are members of a national controlling body, especially those that are most likely to act in unethical ways. Finally, industry boards or associations can only provide guidelines and have no power to enforce compliance (Katzenstein & Sachs, 1992:73).

The above-mentioned limitations lead to a situation where self-regulation alone does not provide an ideal solution to the privacy dilemma. Despite increased privacy guidelines and improved ethical codes observed by marketing industries worldwide, consumer information privacy concerns have increased. From an economic perspective, this can be seen as a market failure and warrants a greater degree of regulation such as government intervention. The next section will address information privacy on a macro level, with specific reference to government intervention by means of data protection legislation.

3. INFORMATION PRIVACY AT MACRO LEVEL

The increasing concern about information privacy is a reflection of, *inter alia*, policy and institutional failure. Policy weaknesses may have major ramifications for consumers and businesses alike and may disrupt perceived economic benefits.

Market outcomes are supposed to be efficient, both allocatively and productively. When they are not efficient, it is considered a market failure and the efficiency rule is violated. All market transactions can be characterised as 'efficient' or 'inefficient', according to whether they satisfy the efficiency rule, namely that marginal benefits to society equal or exceed marginal costs to society. All market transactions should be measured against this rule to indicate how they deviate from it. Given the potential for market failures, it is unlikely that the socially optimal level of economic growth and welfare will be maintained. Therefore, there is a *prima facie* case for government intervention either to correct these failures, or to mitigate their effects and thus improve the efficiency of the economy - the rationale being that a productive economy creates larger incomes, which can be used towards the achievement of other social goals (Mrozek, 1999:412). It is important to note, however, that even when there is a *prima facie* case for government intervention, it may not always be the most efficient course of action to improve a situation and reduce market failures.

In the event of market failures, the economic system is productively and allocatively inefficient. When governments intervene in the market system, they have four basic tools to change economic outcomes, namely taxation and subsidies, public sector production, anti-trust legislation, and regulation. This section will focus on the last tool, namely regulations that require businesses and individuals to behave in certain ways. Economics divide regulations into two types, namely social regulations and economic regulations. Economic regulations are laws aimed at trying to maintain relatively competitive markets. Social regulations are laws that regulate the behaviour of individuals and businesses, such as safety standards and non-discrimination laws.

To promote economic growth, a government can decide to set standards, and maintain and strengthen the legal system. In doing so, it has an important role in providing a social virtue, which is crucial to economic prosperity (Reinert, 1999:273). The information privacy issue cuts across both of these types of regulation. Firstly, economic regulation contributes to creating a competitive global environment when countries adhere to universally accepted international privacy standards. Without compliance, participation in the global market is severely restricted, with a concomitant negative impact on national economic growth. Secondly, social regulation creates an environment that protects consumers from privacy violations by businesses, thus leading to increased consumer trust and confidence in data practices.

The solution to a market failure should be economically sustainable and enhanced economic growth. Economic sustainability is defined as "economic development that meets the needs of the present without compromising the ability of future generations to meet their own needs" (WCED, 1987:8). Pearce and Warford (1993:49) reformulated the above definition as "development that secures increases in the welfare of the current generation provided that welfare in the future does not decrease". A just economy therefore needs to meet the demands of efficiency. An economy cannot be just if, by the nature of its workings, it creates market failures. A new kind of government entrepreneurship is thus required to communicate the objective of creating an efficient economic environment. This environment should guarantee the protection of consumer information.

Good governance implies the inclusion and representation of all the stakeholders in society as well as accountability, integrity and transparency in all government actions. Capable management requires a capacity to fulfil public responsibilities with knowledge, skills, resources and procedures that draw on partnerships. The government should provide both the public and business with the chance to express their views so as to encourage and strengthen partnerships. However, encouraging participation requires the government to have regulatory structures in place that minimise transaction costs and adhere to international best practices (World Bank, 2000:46).

Efficient strategies and complementary policies, linked with consumer involvement, private-sector commitment and accountable government, can ensure a greater prospect of sustainable economic growth. The use of opportunities that present themselves and the exploitation of an area's economic potential, while simultaneously mastering social responsibility and economic challenges in a sustainable manner, are some of the major tasks awaiting governments. Whether this economic potential is realised depends fundamentally on the quality of management and the policies affecting it. The role of the government should be refocused to support markets, communicate a commitment to align policies towards the protection of consumer information, promote economic and social stability, and ensure equity.

The next section, namely information privacy at global level, will provide an overview of government regulation in respect of data protection in other countries.

4. INFORMATION PRIVACY AT GLOBAL LEVEL

Globalisation conveys the widely accepted idea that we are living in a borderless world. According to this view, globalisation signifies the end of geography. No notice is taken of distance or national policy any longer, and national governments must accommodate what global markets dictate (Veseth, 1998:21). On the political map, the boundaries

between countries may be very clear, but on the competitive map that shows the flows of financial and industrial activity, such boundaries have largely disappeared. Competitive nations are those that have chosen correct and well-functioning institutions and policies to promote long-term growth.

The flow of information is playing a major role in eliminating boundaries between countries. National economies are no longer immune from external influences and cannot be insulated against global effects. 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. In an era of globalisation, a country must be competitive both domestically and internationally. If countries want to exploit the benefits of trade and globalisation, they must provide an efficient and attractive place to do business.

Privacy, and specifically information privacy, is currently on the public agenda of many countries (Holvast, Madsen & Roth, 2001:14). The importance of personal data protection has increased to a level where governments and international organisations around the world have been forced to adopt privacy legislation and multilateral instruments. 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). The European Union Directive illustrates how the global marketplace can create a global regulatory environment. Increasing global interdependence has possible consequences for businesses that rely on the unimpeded flow of personal information and that do not protect consumer information to the extent prescribed by European standards (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 countries have joined the 'data-protection club'.

South Africa is currently lagging behind the rest of the world in terms of data protection, despite legislative actions that have been taken by the South African government. The possible consequences that a lack of proper data protection may have on South African businesses can be explained by the following situation. In South Africa, there are currently no provisions by which a company must abide with regard to the use of personal data gathered from its customers during interactions. However, Australian law, specifically the Privacy Amendment Act of 2000, provides that personal information cannot be collected without the consent of the person giving the information. It further provides that the information must be kept confidential and 'cannot be transferred to another country that does not have privacy protection'. This provision means that a South African

company's Australian subsidiary cannot transfer the information it collects from consumers in Australia to the South African parent, since there is no proper privacy protection in South Africa. Likewise, European rules forbid the transfer of personal data to a country that does not provide a level of protection similar to its own. Therefore, the prospect looms of South African companies being denied access to information from their own European subsidiaries or other companies located in Europe (Fjetland, 2002:56).

The information privacy challenge to South Africa will mainly be to find a proper balance between the different competing social and economic interests when drafting legislation. Firstly, the individual merits proper protection in terms of his/her information privacy. Secondly, the Constitution recognises every person's right to engage freely in economic activity and in order to exercise this right properly, individuals and businesses need information about one another. Finally, the government and the private sector can fulfil their functions properly only if they also keep a record of sufficient personal information regarding their subjects (Neethling, Potgieter & Visser, 1996:306).

One of the first challenges comes from the Promotion of Access to Information Act that compels all South African businesses to produce manuals containing the information that is held by them. Several extensions of the deadline for the manuals illustrate that South African businesses are not yet geared to hande information privacy issues as part of their daily managerial tasks (Ivans & Duval, 2002). Future legislation will have to accommodate all these rights and interests in a balanced manner. The aim is thus to address the protection needs of consumers, the financial interests of businesses, and the trading needs of global businesses.

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 economic implications, particularly when the country fails to comply with existing global regulations (Rudraswamy & Vance, 2001:133). The next section will discuss the managerial implications of the information privacy issue together with possible actions needed to reduce information privacy concerns among consumers.

5. MANAGERIAL IMPLICATIONS

Many believe that information will be the heart of the 21st century information revolution, just as electricity was the heart of the 20th century's technological revolution. Technology provides an invisible, automatic means of collecting and analysing consumer data for the construction of consumer profiles. This invisibility may compromise consumer privacy since most consumers do not realise that their information is being collected and used

to construct profiles (Franzak, *et al.*, 2001:637). If a business wishes to set a standard of leadership, it will need to have high standards of respect for personal information, communicate it to all its customers, promote the privacy policy as a competitive edge and make sure compliance is seamless.

To this end, consumers and marketers will in future need to be better educated in what is and what is not acceptable. At industry level, it is important for consumers to be made aware of their rights. What constitutes acceptable and unacceptable behaviour in terms of data collection, utilisation and disclosure by businesses should be communicated to all stakeholders. Additionally, consumers need to know how to protect their information, how to query information held on a business' database and how to remove their information if they so desire (O'Malley, *et al.*, 1999:441). By giving consumers a voice to raise and resolve concerns over their privacy, businesses can increase consumer confidence by establishing a privacy dispute resolution programme.

Businesses, on the other hand, will have to protect consumer privacy and be accountable with regard to their processes of collecting and using personal information. To control consumer information effectively, marketers need to communicate privacy standards to consumers and employees, educate employees, and eliminate the indiscriminate use and careless trading of information (Schwartz, 1998:51). The best way to do this is through a measurable, unambiguous process that emphasises accountability. Many businesses employ Chief Privacy Officers (CPOs) who are responsible for setting privacy guidelines and privacy policies, and ensuring compliance with privacy legislation.

In a less trusting environment, businesses are challenged to balance the creation of value and risk. Privacy policies alone do not earn consumers' trust or their business. Businesses looking for active participation – purchasing goods and services, sharing personal information, and referring family and friends – need to do more than merely provide consumers with their privacy policies. The debate on privacy legislation distracts many businesses from the core issue of privacy as a matter of trust between the business and the consumer. Businesses that wait for regulations to be imposed instead of proactively taking action may not be satisfied with the results. It is likely that regulations will require more activities that do not directly contribute to a trusting relationship with consumers. And waiting for regulation is just a further signal to consumers that businesses are unlikely to protect their data unless mandated to do so.

Given the diversity of business models today and the prevalence of outsourcing, it is no longer enough for businesses to manage the privacy practices only within their own walls. Businesses must also manage the chain of trust they create when sharing customer information with service providers and partners. Businesses have to weigh the cost of

addressing and communicating these consumer trust issues against the return they expect from increased consumer confidence in their privacy practices. Many businesses address privacy to minimise the costs associated with defending the company against privacy lawsuits. However, companies should invest in privacy to obtain a more positive return on their investment - increased revenue and active participation of consumers - rather than just avoiding the risk of potential litigation. Maintaining and growing the business require the preservation of loyal customers, the attraction of new markets, the retention of high-performing employees, and the continuation of successful relationships with consumers. Effective customer relations now require businesses to communicate in ways that make their customers feel protected, and this includes the development of privacy protection policies and the avoidance of inappropriate sharing of customer information.

6. CONCLUSION

Consumer information privacy is becoming an urgent issue of the 21st century and impacts on different levels of marketing and economic activity. Marketers need consumer information as part of their economic activities, whereas consumers express the need to protect their personal and social interests. Businesses need to develop privacy protection policies and communicate these to their customers. A well-designed strategy for communicating the goals and objectives of a business's privacy policy should be based on a deep-rooted understanding of the privacy protection concerns of consumers as well as the laws and regulations affecting the organisation.

Globalisation is forcing countries to implement relevant privacy legislation and comply with internationally accepted privacy codes and standards. The conclusion drawn is that no business, industry, government or country can address information privacy in isolation. It requires a multi-faceted approach involving a combination of communication, education, self-regulation, legislation and international economic cooperation. Businesses should thus communicate their commitment to privacy policies to consumers, join industry self-regulatory programmes and work with government agencies to ensure proper privacy protection.

References

AGRE, P.E. AND ROTENBERG, M. 1998. Technology and Privacy: The new landscape. Cambridge: MIT Press.

ANON. 1999. Privacy promise made to American consumers. *Direct Marketing*, 62(5):6.

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.

CULNAN, M.J. 1993. How did they get my name? An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly*, 17(3):341-362.

DAVIS, J.F. 1997. Property rights to consumer information. *Journal of Direct Marketing*, 11(3):32-43.

DEVENISH, G.E. 1999. A commentary on the South African Bill of Rights. Durban : Butterworth.

FJETLAND, M.J.D. 2002. Global commerce and the privacy clash. *The Information Management Journal*, January/February:54-58.

FLETCHER, K. AND PETERS, L. 1996. Issues in customer information management. *Journal of the Market Research Society*, 38(2):145-160.

FRANZAK, F., PITTA, D. AND FRITSCHE, S. 2001. Online relationships and the consumer's right to privacy. *Journal of Consumer Marketing*, 18(7):631-641.

GLAZER, R. 1991. Marketing in an information-intensive environment: Strategic implications of knowledge as an asset. *Journal of Marketing*, 55(October):1-19.

HOLVAST, J., MADSEN, W. AND ROTH, P. 2001. The Global Encyclopedia of Data Protection Regulation. Supplement No. 3. Netherlands, The Hague : Kluwer Law International.

IVANS, D. AND DUVAL, C. 2002. DMA legal BRIEF. [Web:] . [Date of access: 20 Aug.]

KATZENSTEIN, H. AND SACHS, W.S. 1992. Direct Marketing. New York, USA : MacMillan.

LONG, G., HOGG, M.K., HARTLEY, M. AND ANGOLD, S.J. 1999. Relationship marketing and privacy: exploring the thresholds. *Journal of Marketing Practice: Applied Marketing Science*, 5(1):4-20.

MARUD, M. 2002. Online directory under fire. *Cape Argus*, 8 February:1.

MROZEK, J.R. 1999. Market failures and efficiency. *Journal of Education*, 30(4):411-419.

NEETHLING, J., POTGIETER, J.M. AND VISSER, P.J. 1996. Neethling's Law of Personality. Durban : Butterworth.

O'MALLEY, L., PATTERSON, M. AND EVANS, M. 1999. Exploring direct marketing. London : International Thomson.

PEARCE, D.W. AND WARFORD, J.J. 1993. World without end. New York : Oxford University Press.

PETERS, L.D. 1997. IT enabled marketing: A framework for value creation in customer relationships. *Journal of Marketing Practice: Applied Marketing Science*, 3(4):213-229.

POUNDER, C. AND KOSTEN, F. 1992. Managing data protection. London : Butterworth-Heinemann.

REINERT, E.S. 1999. The role of the state in economic growth. *Journal of Economic Studies*, 26(4/5): 268-326.

RUDRASWAMY, V. AND 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): 127-136.

SCHWARTZ, D.O. 1998. Sharing responsibility for e-commerce and the privacy issue. *Direct Marketing*, 61(2):48-52.

VENTER, Z. 2002. Telkom customer privacy case settled. *Pretoria News*, 20 February:3.

VESETH, M. 1998. Selling globalization: the myth of the global economy. London : Lynne Rienner.

WALCZUCH, R.M. AND STEEGHS, L. 2001. Implications of the new EU Directive on data protection for multinational corporations. *Information Technology & People*, 4(2):142-162.

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

WESTIN, A.F. 1995. Privacy in America: An historical approach and socio-political analysis. Presented at National Privacy and Public Policy Symposium, Hartford.

WORLD BANK. 2000. World Development Report. Entering the 21st Century. New York : Oxford University Press.

WORLD COMMISSION ON ENVIRONMENT AND DEVELOPMENT. 1987. Our common future. Oxford : Oxford University Press.

YUDELSON, J. 1999. Adapting to McCarthy's four P's for the Twenty-First Century. *Journal of Marketing Education*, 21(1):60-67.