South African Journal
of Information Management
[DoE accredited]

Peer Reviewed Article Vol.4(1) March 2002

Customer-centric data warehousing in organizations and the privacy of the individual as a customer: a call for re-examination

S.R. Ponelis
Department of Information Science
University of Pretoria
sponelis@hotmail.com

J.J. Britz
Department of Information Science
University of Pretoria
Britzh@postino.up.ac.za

Contents

1 Introduction

In a global information-based economy, data about customers are one of the most important sources for competitive advantage. As one of the research associates from the London-based think tank Demos states: 'We produce and manipulate personal information on an industrial scale. Personal data are the fuel of the modern economy' (Pink 1997:58). Hagel and Rayport (1997:53) also indicate that 'information about customers enables organizations 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 and services'.

The ability of an industry to capture, collate and analyse personal data, both demographic and transactional, indicates that the resulting databases can pose a significant threat to individual data privacy protection. This threat to privacy was already anticipated in 1977 by

the US Privacy Protection Study Commission (USPPSC 1977). Furthermore, the merging of data from disparate sources poses a threat to privacy because information from a variety of databases can be integrated into a central database. Also, individuals are often not aware of personal information being integrated into a central database. The individual is quite possibly unaware of the purpose or purposes of the integration, the identity of the agency that implemented the integration and the identity of the benefactor of the created database. Whether the information is accurate, is also an aspect that the individual has no knowledge of (Britz 1999:298).

Although consumers are becoming increasingly edgy about the amount and depth of information businesses collect about them, Brown (1997:219) urges that the general public and its advocacy groups should be asking privacy-related questions with far more urgency and persistence. There is also a lack of knowledge and understanding on the part of individual customers, who comprise the public, of what organizations are capable of doing with information technology and how their personal data are used, with particular reference to data warehousing. Organizations, on the other hand, have not always been forthcoming in revealing this to the public in general or their customers in particular.

top

2 Scope

Against the above background, this article reports on the rise in importance of the customer and his or her data to organizations. The article further reports on the role of data warehousing within organizations and how it can threaten the right to privacy of the individual as a customer. Thereafter, the authors argue for a re-examination of the development approach of data warehouses in line with privacy principles in order to mitigate some privacy concerns.

The government, as either data collector or legislator of the relationship between the data subject and the data collector, is excluded from the scope of this discussion, as is the different approaches to privacy at a macro-level, for example legislation and voluntary compliance to sectoral codes. The implications for data security are not explicitly addressed, but it is assumed that the importance of adequate security for all organizational data is accepted, in particular for data concerning individuals.

top

3 Assumptions

Data warehousing is a process for constructing an information technology system that supports business processes and strategy. To achieve this, a solution may be sought either through the business processes that warehousing supports or through the underlying technology of warehousing itself or a combination of both. Although business processes are to some extent generic in terms of accomplishing similar tasks, they have to be specific to an organization's particular strategy. However, the modification of business processes or strategy is not included in this discussion.

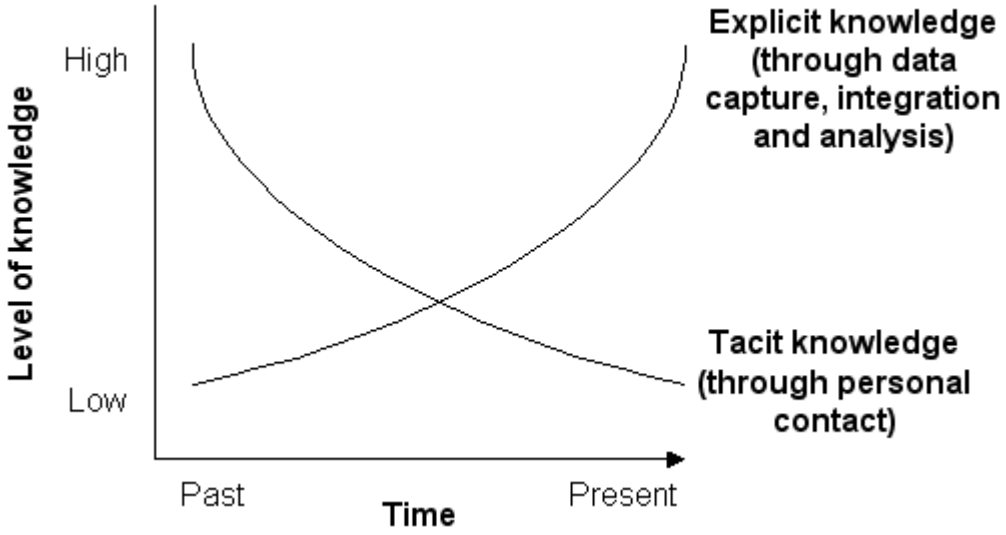
The authors assume the individual's right, both legally and ethically, to privacy. The resolution of the individual's right to privacy through non-technological means and the economic imperative for infringing on this right are not discussed. Following from this, the way in which individuals perceive privacy, for example as a right or as a commodity, as well as the reasons behind their perceptions, is also excluded.

top

4 Recognition of the business value of customer data

The source of an organization's knowledge about its customers has changed. Years ago a shopkeeper knew his or her customers through personal contact. This model of tacit knowledge through personal contact has become impractical since it cannot scale beyond a local level. For a regional, national or global organization, this tacit knowledge must be substituted by explicit knowledge obtained through capturing customers' transactional and personal data. Figure 1 depicts this schematically.

Figure 1 Change in the source of an organization's customer knowledge over time



4.1 Customer-organization relationship is a form of intellectual capital

Skandia, a Swedish insurance company, developed a model for accounting intangible assets or intellectual capital. Customer capital forms part of structural capital, which together with human capital constitutes intellectual capital (Edvinsson 1997:369). Wiig (1997:401) furthermore states that customer capital is the value of the enterprise's relationships with its customers. Roos and Roos (1997:416), however, categorize intellectual capital as human capital, organizational capital and customer relationship capital. In their study of intellectual capital in Scandinavia, they found that 'relationship capital was the most important necessary factor for success' (1997:417). Whichever way intellectual capital is subdivided, it is clear that knowledge about customers and a relationship with them form an integral part of an organization's intellectual capital.

4.2 From mass production to mass customization

The move from mass production to mass customization has led to changes in the nature of the relationship between the organization and its customers. According to Samarajiva (1998:278) there is a trend to move away from mass production to mass customization. This trend is especially strong in service-related, communication intensive industries as it satisfies the different needs of the market more effectively.

An important implication of this shift is the world economic system's transformation from a dominantly mass production model to a mass customization model. This creates an enormous demand for detailed personal-related data on the behaviour of consumers. Owing to this demand even hitherto anonymous transactions are now converted to information-yielding relationships. Frequent-shopper programs exemplify this even further (Samarajiva 1998).

4.3 Customer relationship management (CRM)

Customers are demanding faster, personal service from organizations. Consequently, organizations must respond to this need to ensure their survival. This need has given rise to customer relationship management (CRM) software. CRM has become a key business initiative for organizations, particularly because of the explosion of customer choice and the constant rise in the customer's expectations of service. The main objective is to cultivate customer loyalty by enabling an organization to establish a relationship with each customer as an individual and differentiate its service and/or product based on personal data gathered from the customer. The customer loyalty is partly a result of the effort expended by the customer in providing data regarding, for example preferences, and locks the customer into a relationship with the organization.

It is clear that customer data have become a valuable organizational asset and resource. As Zuboff (1996:13) states: 'In an information economy, information is the core resource that firms exploit in order to create the value their customers seek.' The aim is to grow revenue by leveraging the data at the organization's disposal, but the success depends heavily on customer data being captured at the desired level of detail.

Capturing customer data, however, is not enough. Organizations have been collecting electronic customer data for years, but it was cumbersome to integrate the data to form an integrated view of the customer (Prahalad and Krishnan 1999:111). Furthermore, Hagel and Rayport (1997:55) remarked that customers have become aware of the ability of companies to collect information but that it far outstrips their ability, or inclination, to deliver meaningful value in return. This gap is widening as companies accumulate huge databases of detailed information about their customers and wrestle with the challenge of mining the data for value.

This lack of integration is mostly due to technological limitations. Advances in information technology (e.g. CRM software) capabilities have made it possible to integrate this data with other data warehouses.

top

5 Using the data warehouse for customer data: the customer-centric data warehouse

A data warehouse is a centralized repository or database used to store integrated data from both internal and external sources. This repository can contain historical data for several years. Data warehouses with a focus on customers are generally referred to as customer-centric data warehouses. These data warehouses are part of the structural intellectual capital required to enable the customer or relationship capital in an organization.

Customer-centric data warehouses are intended to support mainly the sales and marketing function in an organization. It is used as the data source for, among other things, customer profiling, promotion and/or marketing campaign planning and analysis, market basket or affinity analysis, customer retention or churn analysis, customer profitability analysis, cross-selling opportunity identification and sales force analysis. Swift (2000) discusses the evolutionary use of data warehousing in a CRM context. This use progresses through three stages, starting with reporting. Even reporting from the data warehouse to determine what happened, mostly through predefined queries 'provides new views and an ability to use combined, cross-organizational detailed data to understand the past' (Swift 2000). The second stage of use is characterized by analysis, focusing on reasons for what happened. The final and most sophisticated stage, also presenting the most competitive advantage, is forecasting what will happen by means of analytical techniques.

5.1 On-line personalization

The emergence of e-business coupled with the speed and interactivity of the Internet is a further imperative for CRM. This is reflected in current popular business literature, such as Tapscott, Ticoll and Lowy (2000:192) who state that the ubiquitous, cheap and interactive Internet, which is connected with enormous low-cost databases, enables producers to develop a meaningful and direct relationship with each customer. Furthermore, 'customer loyalty is at a premium on the Web, where convenient site access and low switching costs promote user promiscuity' (Brito 2000:5).

Organizations are undertaking aggressive customer loyalty initiatives with the most popular approach to achieve greater loyalty by personalizing the customer's on-line experience with customized products, services and content. Personalization differs from customization. Customization occurs when a customer indicates his or her preferences explicitly and data is provided accordingly; personalization is primarily based on information that companies and vendors have gathered about consumers, such as their purchase history or the Web pages that they have viewed (Stellin 2000:15). It is no longer sufficient to analyse site activity. A visitor's activity and information about on-line behaviour must also be analysed through new technology. This has led to the coining of the term 'Webhouse' (Kimball and Mertz 2000:15) for a Web warehouse, where the data generated through customers' interaction with the organization's Web site are stored. According to Stellin (2000:15) the challenge for companies that are experimenting with personalization will be to provide services that their customers want, but without appearing to know too much about them and thereby risk scaring them away.

5.2 Granularity

In the context of this article, granularity is the level of detail of data needed to describe customers (Kurtyka 1999). To ensure more granular data where it is not inherent to the data, organizations utilize loyalty programmes, for example frequent shopper cards with incentives for customers to use during transactions.

With the introduction of Extensible Markup Language (XML) on the Web, Kimball and Mertz (2000:13) believe that its widespread use will eventually increase the granularity of the clickstream. The reason is that a low-level record could now consist of an action taken against an individually named field on a page rather than the whole page.

However, the arguments against highly granular data primarily refer to cost, storage capacity and/or maintenance - not privacy:

'There is a trade off between the cost of granularity and its usefulness. It costs more to collect and maintain data at a very granular level, and this cost has to be balanced against the value that additional granularity can deliver to marketing analysis' (Kurtyka 1999).

Kimball and Mertz (2000:322) remark that if the business analytical needs allow it, granularity can be reduced to cut down the size of the data warehouse, and thereby lower its cost and simplify its maintenance.

5.3 Data quality

Another major issue is that of data quality (Mathieu and Khahil 1998). From a marketing perspective, data quality equates to the accurate representation of the interactions of customers with the company's products and distribution channels and thereby contributes to create a positive relationship between the customer and the company. In 1996 Wang and Strong (Mathieu and Khahil 1998) identified four dimensions of data quality together with 15 measurable attributes that are also applicable in the context of customer-centric data warehouses. They are the following:

- Intrinsic data quality (accuracy, believability, objectivity, reputation)
- Contextual data quality (value-added, relevancy, timeliness, completeness, appropriate amount of data)
- Representational data quality (interpretability, ease of understanding, representational consistency, concise representation)
- Accessibility data quality (accessibility, accessibility security).

5.4 Inter-organizational data sharing

Organizations have the need to share their data with other organizations, for example in joint business initiatives or partnerships and in buying and selling of data. Inter-organizational data exchange are said to have many business advantages, such as strengthened relationships and a common market strategy between complementary products and services (Johnstone 1998:6). It will further ensure that partners can work together to sell a value-added product that they would not be able to provide alone. This enhances not only value to the customer, but also promotes the vendor brand and generates revenue for the company (Connors 2000).

Given the consolidation of customer-related data in the data warehouse, organizations may not be content with the range of data available. Therefore they may augment this with external data bought from a third party or shared by a business partner. The data can be demographic or expand the transactional history of the customer to allow for more detailed segmentation and/or profiling. The inter-organizational data exchange of customer-related data can remain restricted, for example in the context of mass customization the customers' preferences, but not their personally identifiable data, need to be communicated upstream in the supply chain.

5.5 Metadata interchange standards

Within the data warehousing and decision support context, XML-based metadata standards are being developed to facilitate data interchange between different decision support tools. This will allow organizations to use different tools to satisfy their various requirements without 'building custom program interfaces or manual intervention' (Marco 2000). These metadata standards will therefore also make it more feasible to share data across organizational boundaries, particularly over the Internet.

top

6 Customer data and customer privacy

The use of customer-centric data warehousing has certain advantages for both the organization and a customer, for example new product development and improvements, marketing tailored to the needs of the individual customer and improved service through an improved customer relationship. The use of personal data (such as demographical and transactional data), however, also gives rise to certain fundamental questions pertaining to the privacy of the individual as a customer and cannot be eliminated by assuming that customers are prepared to disregard these questions in order to receive the (perceived) benefits.

Definitions for privacy have been and continue to be difficult, but it is clear that information and communication technologies (ICT) changed the focus from a situation of isolation of the individual to a situation where the individual requires retention of control: 'Privacy is the claim of individuals, groups, or institutions to determine for themselves how, when and to what extent information about them is communicated to others' (Holdsworth 1999) or, put more strongly, privacy is 'the right to control information about oneself, even after divulging it to others. This component acknowledges the critical value of being able to step forward and participate in society without having to relinquish all control over personal

information' (Center for Democracy and Technology 1995).

The first question therefore is to what degree the individual customer loses control over his or her personal data when the data become customer data in the organizational domain: 'The ability of individuals to control their personal information is perhaps seen as the major privacy issue' (Privacy International #A19). The customer also no longer knows who has his or her personal data and how and for which purpose the data are used. As Volokh (2000:85) states, the customer is increasingly the object of his or her own data, but not the subject of the communication of this data.

The second question pertains to the accuracy and reliability of the customer's personal data. It covers issues such as contextual integrity without which the context for understanding and interpreting the information is lost (Britz 1999:299), the nature and use thereof, the acceptance of responsibility for verification and the right to access to this data. The use of inaccurate and unreliable customer data, that is data with a low intrinsic data quality, for decision-making has a twofold impact on the organization. Firstly, the decisions regarding product development, marketing and service delivery would be based on incorrect information and, secondly, an incorrect outcome could result when an organization uses the personal data to make a decision that affects the customer as an individual, for example when a credit bureau provides incorrect data to an enquiring organization, it will cause the rejection of the credit application from banks, retail stores, etc. This affects the autonomy of the individual and can result in information discrimination (Van Den Hoven 1997:35-36). The problem is exacerbated in cases where the customer is not informed of the reasons for the decision and/or is not allowed to access his or her personal data used in decision-making.

It is clear that customer-centric data warehousing can hold serious implications for the privacy of the individual and therefore also for core human values such as freedom, autonomy and security (Moor 1997:28). Existing legal frameworks do not adequately protect the individual in this regard - it is not the data that are 'in need of protection; it is the individual to whom the data [relate] (Mayer-Schönberger 1998:219). Furthermore, data protection also does almost nothing to prevent or limit the collection of personal-related information. According to Davies (1998:156), data protection merely stipulates that personal-related information has to be collected by lawful means and for a purpose directly related to a function or activity of the collector. This implies that databases, including data warehouses, that collect data for legitimate organizational functions such as marketing, can be built without impediment and/or breach of law.

Customer-centric data warehousing, therefore, cannot function solely within an economic-based exchange relationship between the customer and the organization, but requires a social contract based on mutual trust and personal obligation. This expression of trust and personal obligation on the part of the organization can be found in privacy principles such as the following from the Joint Legislative Task Force on Personal Information and Privacy, which is based on the principles of the Privacy Rights Clearinghouse, which in turn were adopted from several existing sets of fair information practices developed since the early 1970s, including those of the United States Department of Health, Education and Welfare Fair Information Practices (1973), the international principles of the Organization of Economic Cooperation and Development (OECD 1980) and the Canadian Standards Institute Privacy Code (1996) (Jones 1998). The basic principles can be summarized as follows:

1. Principle of proactivity: According to this principle, privacy implications must be recognized explicitly. It must be considered when personally identifiable information is being used.

2. Principle of secondary use: Personal and private information must not be disclosed or used

for any purposes other than that for which it was collected. Secondary use of personal and private information is permitted only with the consent of the individual.

3. Principle of access: An organization has the obligation to make specific information available to individuals about its policies and practices relating to the handling of personal and private information. Individuals must also have reasonable means to learn about, access, review and, when necessary, correct information about themselves.

4. Principle of affirmative consent: According to this principle, the consent of the individual is required for the collection, disclosure or use of personal information.

5. Principle of relevance: The collection of personal and private information must be limited to that which is necessary for the transaction with the individual and purposes identified by the organization. The specific purpose for which personal information is collected must also be specified. Personal and private information must also not be retained longer than necessary for the fulfilment of the purposes.

6. Principle of accuracy: Personal and private information must be accurate, up to date and complete. It must also be reviewed on a constant basis.

7. Principle of security: Reasonable safeguards must be taken to protect personal and private information against the risk of unauthorized collection, access, use, disclosure or disposal.

8. Principle of accountability: An organization is responsible for personal information under its control. An individual must be able to challenge compliance with the above principle with the organization.

9. Principle of progress. As information technologies develop, privacy considerations are likely to change. These principles must therefore be reviewed on a regular basis to ensure their sufficiency and adequacy.

Hagel and Rayport (1997:54) state that those companies and vendors that do the best job of using information to provide value to customers will eventually be in a position to gain access to more information. Organizations need to recognize that addressing these fundamental questions surrounding privacy of customers' personal data is an integral part of 'doing the best job'.

top

7 Re-examining the approach to data warehousing

Based on the principles related to privacy as outlined above, particular aspects of the development and use of data warehousing call for discussion. These aspects are related to the relevant privacy principles in order to begin addressing the fundamental questions. This is not intended to be a comprehensive discussion, nor a definitive solution. Rather, the purpose is to indicate the relevance of privacy to data warehousing and stimulate further debate and research in this area.

Referring to the principle of proactivity, it is clear that this is an area of concern in customer-centric data warehousing. This is particularly relevant given the general approach to the development of databases in organizations: 'Without intending to cause harm, firms that haphazardly implement database technology without sufficient regard to privacy implications pose a far greater danger [than the possible illicit uses of stored data]' (Debord 2000). While the intentions of the firms remain open for debate, the statement raises a valid point.

Furthermore, there are concerns that the privacy safeguards are too often not 'built-into' the development of technology, but are 'bolted-on' as a later and less effective appendage (Privacy International #A13). However, as Riley (1995) argues, interoperable systems and the greater attention to data and information management need not spell danger to privacy protection, that is, if such systems are designed with privacy and security in mind. The new developments in technology can also be used to allow for better privacy protection features to be built in from the outset (Privacy International #A24).

Unfortunately, privacy and security measures have not been integrated on a large scale into systems development life cycles (Riley 1995). Although there are specific instances where privacy concerns of data subjects have been incorporated into a system's development life cycle and various development methodologies (e.g. the use of privacy impact assessments), this has not been the generally accepted practice. However, this historical practice does not give justification for continuing to do so in the future. The need to address privacy and security in a comprehensive manner in all instances of development is clear. This would also pertain to the development methodologies used for data warehouses and customer-centric data warehouses in particular.

An example of how this would translate to practice relates to the customer verification of data. In line with the principle of accuracy, it is in the interest of the organization to have high quality data on its customers. Furthermore, the business value of allowing customers access and control, albeit limited, over their data is increasing. Using the Internet, organizations can allow customers access to their data contained in the data warehouse to verify that the data are accurate. The security considerations must, however, be taken into account when addressing the intrinsic and accessibility dimensions of data quality mentioned earlier. The principle of access will then also be adhered to. Making corrections, however, is not such a simple task and can be seen as a major concern for the protection of the customer's right to be presented in the correct way. According to the definition of a data warehouse, direct updates should not be allowed to take place, but rather in the source systems to ensure data integrity. As Kimball (1996:xxvii) states, the data warehouse 'cannot fix poor quality data'. The only way to fix poor quality data is to return to the source of the data with better systems and better management.

There are some strong arguments for consolidating personal data, including demographics and credit information, into one location within the enterprise. These arguments are based on the following reasons (Kimball and Mertz 2000:126):

- Access to information can be better controlled and audited if the information to be protected is in one location and not distributed throughout the enterprise.
- It is relatively easy for Web sites to respond quickly to changing legal requirements for privacy control.
- A user's access privileges to controlled content can be monitored and granted on an enterprise-wide basis when it is needed.

This assumes that data are captured directly in the data warehouse and do not reside in other source systems. While this is not the reality in most customer-centric data warehouses, the situation will have the benefit of allowing users not only to verify their data by accessing the data warehouse, but also to update their data as there are no source systems in which the correction(s) must be made.

Riley (1995) furthermore remarks that an essential first step in the modified systems development process is to make sure that there is a wider group of interests involved in the planning, steering and approval of personal information systems. In the context of participatory design (PD), which refers to the relation between the system designer and the

user of the system, Kensing and Blomberg (1998:172) state that the development of meaningful and productive relations between those who are charged with technology design and those who must live with its consequences is of specific importance. Korpela et al. (cited in Kensing and Blomberg 1998:173) also argue that not only end-users must be involved, but also community members who will be served by the system. This indicates that the approach of participatory design should be examined to ascertain whether it could contribute to the process by involving the data subjects in the construction of the customer-centric data warehouse. In the same manner that user participation and buy-in is a critical success factor in the acceptance and use of an information system, participation of the customers, as the data subjects, must become critical to the success of system.

In the PD context, users can have different levels of influence on the design of a system (Bratteteig 2000). These levels of influence could also be applied in the context of customers' involvement in the development of a customer-centric data warehouse as well as their becoming members of the project team. The least influential of these levels entails informing customers about the decisions that are made regarding the data warehouse. The next progressively more influential levels are for customers to be consulted and allowed to express their opinions, having representation in the steering board and/or the project group and cooperating and participating in the project itself. This approach might, however, result in increased complexity, more costs and a longer development time frame, and can be met with resistance from both organizations and their development teams.

As an initial alternative, the authors suggest the creation of a full-time role in the data warehouse project team from the outset to focus solely on privacy-related matters. This person should preferably be independent of the organization or, in cases where a vendor or consulting firm is retained to construct the data warehouse, independent of such vendors or consulting firms. This will ensure the best interest of the customers' privacy. This person could be representative of a privacy auditor ultimately answerable to the customers, or a representative of a consumer advocacy group nominated because of his or her knowledge and concern. As with the approaches in participatory design, organizations and development teams might also question the feasibility of this approach. An employee of the organization whose job function is solely focused on privacy-related issues and who is accountable to customers in this matter (as would be suggested according to the principle of accountability) could be a compromise solution. Once again, if the process used is not transparent and inclusive, the positive intention to gain the trust of the data subjects will result in a negative perception of the organization. This alternative should also not be seen as a reason to overlook the participatory possibilities mentioned earlier.

In accordance with the principles of affirmative consent and relevance, and countering the basis for on-line personalization, Holdsworth (1999) suggests the possibility of a Web-based standard. Such a standard will allow organizations and individual consumers to interact with data collectors and inform them of the information they would comfortably have disclosed to other individuals and companies. The World-Wide Web Consortium (also known as W3C) is developing such a standard as a specification called the Platform for Privacy Preferences Project (P3P). This specification will enable Web sites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents. P3P user agents will then inform users of site practices (World-Wide Web Consortium 2000). It must be noted, however, that 'although P3P provides a technical mechanism for ensuring that users can be informed about privacy policies before they release personal information, it does not provide a technical mechanism for making sure sites act according to their policies' (World-Wide Web Consortium 2000). Should a standard such as this become a reality and attain critical mass with on-line customers, organizations capturing customer-related data from the Web will have to take the standard into account in the modification of existing data warehouses and the building of new ones (or new 'Webhouses').

The question of how to handle already captured historical customer-related data will also need to be addressed. Another pertinent question is how organizations should handle personal data captured under a particular privacy policy after the privacy policy has been changed, for example as the on-line bookseller Amazon has recently done (Waldt 2000:26).

Compliance with the stated organizational privacy policy is a major concern based on the principle of accountability. The development of a generally accepted set of privacy principles will greatly assist in enabling the protection of individuals' privacy, given that these principles are fair. The responsibility for setting the standards and/or principles is, however, a very pertinent issue. If this process is not transparent and credible, the customers will lose their trust in the organization.

Data warehouses should be audited for public notification to certify compliance with privacy principles. Privacy auditors, who are trusted third parties in the relationship between the individual as customer and the organization, can do this auditing. Already organizations, from consulting to law firms, are offering many such privacy-related services to organizations. These services include identifying privacy implications of existing or proposed business operating procedures, legal advice regarding compliance with regulations and laws, development of an organizational privacy code or policy, developing programs for internal compliance to these policies or codes, privacy audits to ensure external compliance and awareness training.

The integration of the ethics related to privacy and the relation between privacy and technology into the curricula of students who are the future users, developers, data subjects and auditors of data warehouses will further help to establish a different approach to the development of organizational customer-centric data warehouses.

top

8 Conclusion

The threat that organizational customer-centric data warehouses pose to its customers as individuals was indicated. While no definite solutions were presented, the purpose of this article was to stimulate the debate regarding organizational data warehousing and the privacy of the individual as customer. An argument was made for the re-examination of the approach to building data warehouses and the data warehousing methodologies used to address these concerns.

top

9 References

Bratteteig, T. 2000. Participatory design: ideas, methods, practices. Lecture presented at the International Women's University, July 27, 2000.

Brito, M. 2000. Analyzing the traffic of the information super highway. *Microstrategy* Magazine (January/February):4-6.

Britz, J.J. 1999. Technology as a threat to privacy. In *Encyclopaedia of Library and Information Science*. Vol. 65. Edited by Allen Kent. New York: ACE Production:295-305.

Brown, D. 1997. *Cybertrends: chaos, power, and accountability in the information age*. London: England: Viking (Penguin).

Center for Democracy and Technology. 1995. Privacy and individual empowerment in the interactive age. [Online]. Available WWW: http://www.cdt.org/publications/ftc_xprivacy_112095.html.

Connors, J. 2000. E-business challenge: keeping sales channels flowing [Online]. Available WWW: http://www.ecomworld.com/html/automate/060100_2.htm.

Davies, S.G. 1998. Re-engineering the right to privacy: how privacy has been transformed from a right to a commodity. In: *Technology and privacy: the new landscape*. Edited by Agre, P.E. and Rotenberg, M. Cambridge, Massachusetts: The MIT Press:143-166.

Debord, M. 2000. On-line books: saving privacy. Review of database nation: the death of privacy in the 21st century. [Online]. Available WWW: http://www.thenewrepublic.com/on-line/debord041300.html.

Edvinsson, L. 1997. Developing intellectual capital at Skandia. Long Range Planning 30 (3):366-373.

Hagel, J. and Rayport, J.R. 1997. The coming battle for customer information. Harvard Business Review (January-February):53-65.

Development of surveillance technology and risk of abuse of economic information (an appraisal of technologies of political control), May 1999 Part 1/4. Edited by D Holdsworth. European Parliament, Directorate General for Research, Directorate A, The STOA Programme. [Online]. Available WWW: http://cryptome.org/dst-1.htm.

Johnstone, K. 1998. The power of information: an article of strategic decision support. Arthur Andersen Data Warehouse Practice Leader (Dallas). September 30, 1998.

Jones, I.C. 1998. California legislative report, California State joint task force on personal information and privacy - held March 3, 1998. [Online]. Available WWW: http://feefhs.org/csga/lr-jtfpp.html.

Kensing, F. and Blomberg, J. 1998. Participatory design: issues and concerns. *Computer Supported Collaborative Work* 7:167-185.

Kimball, R. 1996. *The data warehouse toolkit: practical techniques for building dimensional data warehouses*. USA: John Wiley and Sons, Inc.

Kimball, R. and Merz, R. 2000. *The data Webhouse toolkit: building the Web-enabled data warehouse*. USA: John Wiley and Sons, Inc.

Kurtyka, J. 1999. CRM: marketing the complex customer. DM Direct. [Online]. Available WWW: http://www.dmreview.com/master.cfm?NavID=198&EdID=1724.

Marco, D. 2000. Meta data and data administration: XML: The global meta data Standard. DM Review. [Online]. Available WWW: http://www.dmreview.com/master.cfm?NavID=198&EdID=1845.

Mathieu, R.G. and Khahil, O. 1998. Data quality in the database systems course. *Data Quality* 4(1). [Online]. Available WWW: http://www.dataquality.com/998mathieu.htm.

Mayer-Schönberger, V. 1998. Generational development of data protection in Europe. In: *Technology and privacy: the new landscape*. Edited by Agre, P.E. and Rotenberg, M.

Cambridge, Massachusetts: The MIT Press:219-242.

Moor, J.M. 1997. Towards a theory of privacy in the information age. *Computers and Society* 27(3): 27-32.

Pink, D.H. 1999. Personal protection. *Fast Company* (February/March):58.

Prahalad, C.K. and Krishnan, M.S. 1999. The new meaning of quality in the information age. *Harvard Business Review* (September-October):109-118.

Privacy principles for California. Draft for discussion purposes. Prepared for the Joint Legislative Task Force on Personal Information and Privacy. Senator Steve Peace, Chair March 3, 1998. [Online]. Available WWW: http://www.privacyrights.org/ar/princip.htm.

Privacy International. Country report: Canada (review of responses to discussion paper issued by industry Canada in cooperation with the Information Highway Advisory Council). [Online]. Available WWW: http://www.privacy.org/pi/countries/canada/report.html.

Riley, T.B. 1995. Living in the electronic village: the impact of information technology in a changing world, PHASE II: privacy vs. openness: satisfying the two. [Online]. Available WWW: http://www.rileyis.com/publications/phase2/privacy.htm.

Roos, G. and Roos, J. 1997. Measuring your company's intellectual performance. *Long Range Planning* 30(3):413-426.

Samarajiva, R. 1998. Interactivity as though privacy mattered. In *Technology and privacy: the new landscape*. Edited by Agre, P.E. and Rotenberg, M. Cambridge, Massachusetts: The MIT Press: 277-310.

Stellin, S. 2000. Internet retailers struggle to master 'personalization'. International Herald Tribune (36542):15.

Swift, R. 2000. The stages of growth for CRM and data warehousing. DM Review. [Online]. Available WWW: http://www.dmreview.com/master.cfm?NavID=198&EdID=2632.

Tapscott, D. et al. 2000. *Digital capital: harnessing the power of business Webs*. Boston, Massachusetts: Harvard Business School Press.

US Privacy Protection Study Commission (USPPSC). 1977. Personal privacy in an information society. Washington, D.C: Government Printing Office.

Van den Hoven, M.J. 1997. Towards a theory of privacy in the information age. *Computers and Society* 27(3):33-37.

Volokh, E. 2000. Personalization and privacy. *Communications* 43(8):4-88.

Waldt, A. 2000. Amazon: Userdaten-Verkauf. de:bug, 040,1000.

Wiig, K. 1997. Integrating intellectual capital and knowledge management. *Long Range Planning* 30(3):399-405.

World-Wide Web Consortium. 2000. The platform for privacy preferences 1.0 (P3P1.0) Specification: W3C working draft 15 September 2000. [Online]. Available WWW:

http://www.w3c.org/TR/2000/WD-P3P-20000915/.

Zuboff, S. 1996. The emperor's new information economy: information technology and changes in organizational work. In: *Information technology and changes in organizational work: working conference proceedings*. December 7-9, 1995. Ed. Orlikowski, W.J. et al. London: Chapman and Hall:13-17.

top

ISSN 1560-683X

Published by InterWord Communications for the Centre for Research in Web-based Applications, Rand Afrikaans University