Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 1995 Proceedings

Americas Conference on Information Systems (AMCIS)

8-25-1995

Association for Information SystemsAmericas Conference on Information SystemsData Privacy and Computer Information Systems

David Mazlin
University of New South Wales

Rodger Jamieson
University of New South Wales, r.jamieson@unsw.edu.au

Association for Information Systems Americas Conference on Information Systems

Data Privacy and Computer Information Systems

David Mazlin - Research Student, School of Information Systems
and
Rodger Jamieson - Senior Lecturer, School of Information Systems
University of New South Wales, Sydney NSW 2052 Australia
Ph: (61) (2) 385-4414/5283 Email: r.jamieson@unsw.edu.au

Introduction

For the last two decades the capacity of computers to store information on an unlimited range of subject matters has increased dramatically. Information held contains both commercial and personal information, some of which is private information and some is available publicly. Unauthorised usage of such information may have financial, political or personal consequences (Hughes, 1991, p83).

The outcome of these threats have been the introduction of legislation and policy guidelines, in many international jurisdictions for both the public and private sectors, to curb the abuse of individuals' privacy. This form of regulation is usually targeted at computer information systems. The potential for abuse of an individual's privacy is highly possible through the use of massive storage facilities and processing capabilities of today's computers. These facilities allow for such processes as: data matching, statistical inference, profiling and dissemination via communication links, to occur.

In Australia, we have been slow to adopt legislation and policy on privacy matters. The only legislative base currently active in Australia that attempts to cover all aspects of personal information privacy is the Commonwealth Privacy Act 1988. This legislation only affects Commonwealth Agencies. There are also certain other organisations that are partially affected by privacy law. The main ones are tax file number holders and credit information providers.

Implementation of such privacy policy and/or law will have effects on the way computer information systems are designed, maintained and audited, and yet little research has been conducted in this area.

Research Methods

This research examines a number of different issues in relation to Australian data privacy legislation and information systems. Four research questions have been identified from literature reviewed in this area, to provide focuses for this research. The research questions are:

1. Do data privacy laws within Australia provide sufficient coverage of International guidelines, to allow Information Systems Practitioners to rely upon them?

2. What problems are encountered by the Privacy Commissioner when auditing Commonwealth Government Agencies for compliance with Australian data privacy legislation?

3. What effects do Australian data privacy legislation have on computer information systems within organisations?

4. What attitudes do personnel of privacy regulated organisations have to privacy?

The research method used to examine these questions was a case study of a medium sized Australian Commonwealth government agency, that deals mainly with personal information. Interviews were conducted within the agency and with some of the Australian Commonwealth Privacy Commissioner's staff. Interviews with 33 people who deal with privacy, and to at least some extent with computer information systems, were conducted. Additional research was carried out through an analysis of privacy audit reports, and review of literature and documents supplied by the government agency and the Privacy Commissioner.

Major Findings

Research Question 1

Current international trends in Europe in relation to privacy provide that if a country does not provide law to enforce an adequate level of data protection, then the country will no longer be allowed to receive transfers of personal information (European Commission: Direction on the Protection of individuals privacy in relation to the processing of personal data). This could have dramatic affects on Australian trade, communications, and professions such as IT professionals in both their professional work practices and in the amount of future work they will receive. To show this adequate level of protection a country must adopt compatible laws, or show an adequate level of protection through other means or exceptions.

The Commonwealth Privacy Act 1988 has been found to provide a level of coverage of privacy that falls below the international standards set by OECD and the European Commission. The proposed NSW Privacy and Data Protection Bill 1994, provides a more adequate level of protection, but still falls short in some regards to the international standards.

Research Question 2

The summaries of the audits and annual reports of the Privacy Commissioner provided data for this research question. The problems from the audits of the Privacy Commissioner were classified in the following categories; information privacy principles (IPPs); general privacy issues; and other areas of compliance within the jurisdiction of the Commissioner. Out of the categories identified, over half of the categories were found as problems in at least 25% of the organisations.

The problems identified were: IPP 2 - incorrect privacy notices on forms (88% of the organisations audited); IPP 4 - not adequate security in the storage of personal information (81%); inadequate privacy training or awareness (69%); IPP 1 - the information needed for a legal purpose related directly to the collector's function (56%); tax file number guideline infringements (44%); IPP 8 - information was not checked for accuracy before use (38%); IPP 11 - personal information was disclosed for reasons outside the stated purpose of collection (31%); IPP 3 - information collection was incomplete, inaccurate, or intrusive (31%); policies relating to privacy were inadequate (25%); and provisions in contracts with external contractors were inadequate to comply with privacy requirements, especially with regards to IPP 4 (25%).

Research Question 3

The Commonwealth Privacy Act 1988 requires that some changes are made to computer information systems in organisations. These changes are influenced by a number of privacy forces, internal and external, on an organisation. The actual changes from within the case study government agency were identified, and the influences for the overall changes identified. Other potential changes were also collected from the case study agency, Privacy Commissioner's personnel, and from implications expressed in the documents reviewed. Some aspects of privacy legislation can be considered as enforcing good information handling practices. Even for the organisations that have these practices in place, at the very least, privacy helps enforce these standards.

Within the case study organisation changes in the information systems were identified; improved IT security, input form design, tax file number handling, links with external information systems, access to live data for testing, data matching, and general systems development. The major direct influences on the information system with regard to privacy were the agency's privacy personnel, privacy regulation, internal audits, and organisational practice and policy. One noticeable influence which was at the bottom of the list was professional organisations. The major privacy influences on internal audits were the risk based approach to audit, agency privacy personnel, privacy regulation, and organisational practice and policy. The privacy influences identified in policy formulation were agency privacy personnel, Privacy Commissioner, and privacy regulations. The privacy influences that effected system users were their training and awareness of privacy, organisational policy, privacy personnel, organisational practice, and social attitudes to privacy. One major conclusion is that it is important to have a

system of privacy in place as it is potentially the highest of the influences within all agency privacy activities.

In addition to identifying the actual changes to the case study agency the study compiled a list of the possible changes privacy legislation could have on information systems. These possible changes relate to the information privacy principles which provide the basis for the Commonwealth Privacy Act 1988. These principles identify four areas of application; collection; storage; usage; and dissemination of personal information. Two major themes run through these principles. The first, is that information must be collected, used, and disseminated for a purpose that is legal and directly connected to the collector's function. The second, is that information upon collection, and before usage, should be checked for accuracy.

The possible changes that an information system can be subject to, due to the provisions of the Privacy Act, include changes in: what information can be collected (IPP 1); input form design (IPP 2); IT security (IPP 4); information stored about personal information records (IPP 5); checking purpose and accuracy before using personal information (IPP 8 and 9); information can only be used for the purpose of collection (IPP 10), reducing such practices as testing on live data, and data matching. Information can only be disseminated for purpose of collection (IPP 11), reducing activities such as links to other organisations as well as the handling of tax file numbers (TFN Guidelines). Other related issues in need of change include policy formulation relating to privacy, and ensuring that outsourcing contracts include privacy provisions (especially IPP 4 - security). There will need to be a responsibility for privacy training and awareness for staff, and changes in certain work practices.

Research Question 4

The attitudes of personnel of a privacy regulated organisation were assessed by personal attitude, perception of agency concern, their level of knowledge, the privacy training and literature provided by the agency, and their awareness of privacy infringements.

Agency personnel considered that privacy was of a high personal concern. Most agency personnel perceived that privacy was of a high priority within the agency. In regards to privacy impacting on the work load of individual personnel, there was in some cases a fine balance in considering the value of privacy to clients versus the procedural problems of privacy and potential problems caused to clients.

The average privacy knowledge of agency personnel was assessed as the minimum level of privacy knowledge needed to carry out the privacy components of their own jobs. The study concluded that auditors, policy managers, user managers, information systems developers, and trainers, should at least have a working knowledge of all of the four basic privacy concepts (collection, storage, use, and dissemination), and a good understanding of the structure of privacy legislation, and knowledge of the contents of information privacy principles. Other personnel should at least have an working knowledge of the basic privacy concepts in the areas related to their current position.

The training provided and the literature provided within the agency could not be statistically shown to be linked with the knowledge level of personnel. This lack of relationship was probably due to analysis and data problems rather than there being no connection. The qualitative data from the study shows that there is indeed a connection.

Conclusion

This study contributes to knowledge by identifying the possible relationships between computer information systems and Australian data privacy legislation; the effects foreign data privacy laws and guidelines are likely to have on Australian laws; the effects these changes are having on IT practitioners; the problem areas in compliance with Australian data privacy legislation; and the attitudes of personnel to data privacy.

Although some limitations were encountered, these limitations were balanced to some degree by the gathering of qualitative and quantitative data from the case study organisation, the personnel of the Privacy Commissioner and from various literature sources.

This study should be of use to IT practitioners who are involved with the identification and solution of some of the problems that will be presented by data privacy legislation. More research into this area will be necessary to support this research and possibly confirm some of the findings and implications proposed by this paper.

Selected References were omitted due to the space limitation

Selected References

Bygrave L A, (1990), "The Privacy Act 1988 (Cth): A study in the protection of privacy and the protection of political power", (1990) Volume 19 Federal Law Review 129.

Hughes G, (1991), "An Overview of Data Protection in Australia", Melbourne University Law Review, Vol. 18, June 1991, p. 83.

Kirby M, (1991), "Computers and Privacy - Established Principles New Problems", The Computer Law and Security Report, May-June 1990-91, p. 25.

Mei P, (1993), "The EC Proposed Data Protection Law", Law and Policy in International Business, Vol. 25, (1993), p. 305.

Smith H J, (1993), "Privacy Policies and Practices: Inside the organizational maze", Communications of the ACM, December 1993, Vol. 36, No. 12, p. 105.