Global Information Privacy Protection and its impact on Business: Some initial findings

Georgia King-Siem
Prof Iain Morrison

School of Information Systems
University of Melbourne
Melbourne, Australia
e-mail: gmksiem@pgrad.unimelb.edu.au
e-mail: iain@staff.dis.unimelb.edu.au

Abstract

As personal data markets expand, regulation is an increasingly important issue for business, governments and consumers. Information privacy protection varies between different jurisdictions at all levels. As trade between jurisdictions increases, pressure to standardize regulation also increases. This trend is already apparent with the possibility of a de facto international standard. This paper looks at the future of information privacy protection and how a number of organizations are adapting to the new regulatory climate.

Keywords

Information Privacy Protection International Standard Business Impact Strategies

INTRODUCTION

This paper is concerned with two important issues; emergence of a de facto international standard for information privacy protection and its impact on business. The first part of the paper considers what geo-political and economic factors are at play and how they influence the emerging de facto standard.

The second part of this paper looks at how this increase in information privacy protection has impacted on several businesses. In particular, how regulatory change has affected organisational awareness, business practices and strategic planning of information privacy.

BACKGROUND

Historically, the definition of personal information or data has been restricted to basic data such as name, date-of-birth, address, social security number, and other basic personal identifiers. Increasing amounts of e-data and greater sophistication in data manipulation has necessarily broadened the definition of personal data to any data that can be linked to a specific individual. For instance, vehicle tracking information commonly used by toll road companies contains personal information concerning individual travel movements. Other information such as security access logs and CCTV records also contain personal information. Using a broader definition, personal data comprises a significant percentage of organisational databases, even those that do not trade in personal data such as where personal data collection is incidental to the main delivery of goods and services. Consequently, information privacy protection is an issue for all organizations, regardless of industry or size.

INTERNATIONAL INFORMATION PRIVACY PROTECTION

Most western and developed countries offer some level of information privacy protection whilst most less developed and developing countries do not. This trend can be associated with the level of technology penetration, the amount of personal data available and general consumerism. As technology becomes more ubiquitous and personal data more widely collected and used, the need for information privacy legislation will increase.

Casual Factors

Legislative reform is usually the result of financial and/or consumer pressure. In the case of information privacy, both consumer and financial interests play large, and not necessarily conflicting, roles. The last ten years have seen electronic records permeate all aspects of everyday life, from financial transactions through to web surfing. The amount of e-data available and the ability to cross-reference that data has inflamed public concern. This

concern has placed, and continues to place, pressure on politicians to protect persons through enacting information privacy legislation that governs collection and (ab)use of personal data.

Financial pressure has arisen in both directions. Understandably, there is resistance to any reforms that impose further obligations on business. Surprisingly, there is also significant financial pressure to strengthen information privacy (Cant, 2001; Reidenberg, 2001; Slane, 2001). Not only does legislative reform improve B2C relations, it also augments Business-to-Business (B2B) trade in and involving personal data. Strong information privacy protection measures reassure consumers whilst facilitating free trade with other jurisdictions.

In 1995, the European Union introduced a new directive (EU Directive 95/46/EC) that set a new benchmark in personal information protection (Reidenberg 2001; Slane 2001; Kirby 1996). Under the EU standard, the transborder flow of personal information is banned with non-compliant countries, constraining trade. As more and more countries adopt the European standard, non-compliant countries are becoming increasingly isolated.

A De Facto Standard

Trade is predicated on custom since, without established rules (customs), trade is risky and ad hoc at best. Custom (jus cogens) is a recognised source of international law. As trade involving personal information (incidentally or otherwise) increases, those customs surrounding its trade become more firmly entrenched. The EU standard is being adopted by more and more nations and thus may become the default custom for international trade involving personal information. As such, it will become the standard for information privacy and may well become enshrined in international law. Many Privacy Commissioners have concluded that such an international standard, or at least a set of principles, is inevitable (Slane 2001).

The exact nature of such an international standard is still open to conjecture. Although many countries have adopted the European standard, the United States has not. Moreover, the US used its economic power to broker a deal (Safe Harbor Agreement) with the European Union effectively exempting it from the European Directive's ban on transborder data flows. Despite this agreement, there is widespread speculation that the US will capitulate and enact its own information privacy legislation (Pedersen, 2002; Reidenberg 2001; Featherly 2001; Slane 2001) due to the limited nature, both operationally and strategically, of the Safe Harbor Agreement.

Irrespective of the US experience and prospects, there is increasing pressure for countries with smaller economies to follow Europe's lead. Countries such as Canada and New Zealand have amended their privacy legislation to meet the EU 'adequacy test'.

From the evidence available, it appears that any international standard in information privacy protection will favour the European standard. For businesses operating within Europe or in European standard compliant countries, any ensuing international standard will have little impact (as it will closely resemble the European standard). For businesses operating in non-compliant countries however, the issue of information privacy protection is increasingly relevant.

In recent years, Australia has amended its Privacy Act in an attempt to meet the European Standard. So far it has failed to do so, but further legislative amendments over the next few years are likely to see Australia meet the standard and establish freer trade with other European standard countries. The next section looks at several Australian based businesses and their experience of, and strategies for, legislative reform in this area.

IMPACT ON BUSINESS

Failure of a particular country to meet the EU standard does not preclude trade in, or incidental use of, personal information by individual businesses. Rather, individual organisations may meet the standard on their own – an often cumbersome and expensive accreditation process.

In the case of national legislative reform, information privacy protection obligations are imposed on all organizations. In an increasing number of countries, organizations no longer have a choice and must comply with introduced information privacy legislation. In Australia, such legislation was introduced in late 2001. A small survey was conducted at that time to assess its immediate impact. Approximately 200 surveys were distributed to a range of organisations with a response rate of just over 20%. The survey questions were loosely grouped into three classes: definitions, current business practices and strategic planning. The results from the survey provided valuable information on how business perceived information privacy as an issue and how it intended to respond to legislative reform. That data was then used to design case studies. The case studies were drawn from the survey respondents based on industry sector, organisation size and age and trading jurisdiction. A total of 8 organisations were selected and most of the case studies are still underway.

The main objective of the case studies is to determine how legislative reform has impacted on the business community. From the research conducted so far, the impact of legislative reform varies most according to organization size. Some initial findings from the survey and three of the case studies are discussed below.

Survey Results

Although the survey found that awareness of the Australian legislation was quite high, actual understanding of what was required by that legislation was not. Moreover, only large organizations, typically multinationals, were aware of information privacy protection overseas. Under the Australian legislation, organizations had three choices: adopt the national privacy principles (NPPs), adopt an approved industry code, or develop their own approved code. Most chose to adopt the NPPs as the easiest and cheapest method of compliance. Almost all viewed the new legislation as a compliance issue and not a business opportunity.

To ensure compliance, most Australian based organizations created a privacy officer role (often incorporated into an existing position). Other structural changes included new responsibilities for security and customer relations personnel. In many cases, this meant developing new accountabilities and chains of command.

On the procedural side, all organizations introduced new privacy policies and procedures. For the most part, these procedures related to the collection, storage and accessibility of personal information. Whilst information privacy does not historically comprise a formal part of corporate strategic planning, it has resulted in several strategic changes to how businesses view information privacy and its management.

Organisation 1 (B1)

Organisation 1 ("B1") is a large private sector national organization with an annual turnover of over one billion Australian dollars. B1 identifies itself as a leisure industry organisation. Although B1 does not trade in personal data, it does have extensive customer databases. Prior to December 21, 2001, there were no information privacy requirements imposed on the private sector.

Awareness: Awareness of information privacy arose in the IT Services Group in the mid 1990's due to media coverage of New Zealand's legislative reform and possible changes in Australia. Early recognition and investigation of information privacy by B1 resulted in the efficient implementation of information privacy policies and procedures throughout the organization by December 2001.

Business Practices: Prior to the legislation, information privacy and any attendant issues were handled by the IT group. As the proposed legislation became more prominent, management picked up information privacy as an issue. Strategically, management created a new 'compliance manager', responsible for all legislative requirements, including information privacy. The compliance manager was drawn from the IT group and had been the main driver of information privacy reforms. In addition to the Compliance Manager, key personnel (IT Security Managers and Customer Relations) were given special training and responsibilities for the collection and use of personal information. Specific contact locations and times were created for personal information enquiries – enquiries that can only be handled by privacy trained personnel.

Strategy: Indicative of its compliance-only view, B1 appointed a Compliance Manager to ensure B1 met its obligations under the new legislation. Rather than trying to create privacy officer roles at each location, the Compliance Manager strategically added privacy responsibilities to IT Managers. Consequently, information privacy protection is becoming part of the corporate culture, reinforced by privacy audits. By constraining access to certain personnel, B1 strategically ensured it met the new privacy requirements with the minimum of cost. Rather than initiate organization wide training and procedural changes, B1 immediately limited information privacy to security and customer relations personnel. This knowledge rich, action poor approach has allowed B1 to meet its statutory obligations whilst keeping privacy costs negligible.

Organisation 2 (B2)

Organisation 2 ("B2") is a small private sector multinational organization with an annual turnover of less than five million Australian dollars. B2 identifies itself as an ICT industry organisation.

Awareness: Due to initial small business exemptions, B2 avoided information privacy protection until the last minute. This was due to both a lack of awareness and financial priorities. Awareness of the new legislation was limited to compliance and possible repercussions (for lack of compliance). Once B2's liabilities were determined, interest and awareness in information privacy protection waned.

Business Practices: B2 has taken a reactive approach to the new privacy requirements with no structural changes and minimal procedural changes. As a relatively small and flexible company, B2 was able to initiate its privacy policies with limited cost. Responsibility for information privacy protection fell to the Board of Directors.

Despite awareness of legislation in other jurisdictions, B2 has chosen to adopt the NPPs as the most expedient means of legislative compliance.

Strategy: B2 identified information privacy as a low priority issue with little return on investment. It had considered overseas legislation, but determined the rate of change as too slow to warrant strategic planning. Indeed, it felt that a reactive approach to legislative reform was more strategic than trying to meet the European standard. B2 trades in Australian and predominantly in the United States and thus is more concerned with U.S. law than European law. After some consideration, B2 concluded it was more cost efficient to adapt its information privacy policies and procedures to Australian law as and when required.

Organisation 3 (B3)

Organisation 3 ("B3") is a medium sized private sector multinational organization with an annual turnover of around ten million Australian dollars. B3 identifies itself as a manufacturing industry organisation. Information privacy only became an issue with the introduction of the new legislation.

Awareness: B3 awareness of information privacy was relatively limited until late 2002. Although aware of the new privacy legislation, B3 was not aware that it had any obligations under the legislation. As it did not trade in personal information and only had a limited customer database, it had assumed that the privacy legislation did not apply. B3's awareness of information privacy changed drastically when it applied for ISO9000 accreditation. Under ISO9000, all relevant legislation must be complied with (which includes the new privacy requirements). This put information privacy high on B3's agenda and new privacy policies and procedures were implemented within 6 months. B3 has now received ISO9000 accreditation.

Business Practices: Although there have been some procedural changes, there have been no structural ones. Rather, responsibility for information privacy protection lies with the General Manager. Divisional managers have also incorporated information privacy into their roles, but there have been few changes to operational procedures. This is largely due to a recent security overhaul that addressed most information security and accessibility issues.

Strategy: Once information privacy protection was recognised as an issue (albeit due to ISO9000), B3 acted quickly to ensure compliance under the legislation. Rather than incur research or consulting costs, B3 chose to rely on a state industry body. Using information provided by the association, B3 adopted the NPPs with minimal cost or impact to the company. For B3, legislative compliance was merely one step towards the more strategic goal of ISO9000 accreditation. To contain costs, B3 relies on industry bodies and business journals for advance warning of any legislative change.

CONCLUSION AND FURTHER RESEARCH:

From the three case studies briefly summarised above, it appears that a reactive rather than proactive approach has largely been adopted. This seems to be due to (a lack of) identified returns on investment and perceptions of low corporate business priority. Most organizations surveyed felt that information privacy was a compliance issue that offered very few business opportunities and thereby treated it as a cost. Only organizations that either traded in or used extensive amounts of personal information took a more proactive approach. Larger organizations also tended to take information privacy obligations more seriously, initiating privacy reviews and audits, no doubt with an eye on corporate branding and protection of reputation. In most of the organizations surveyed to date, responsibility for information privacy protection was distributed across several existing positions. This approach was selected predominantly to minimise cost, with the offsetting benefit of embedding responsibility for privacy policies and procedures into organisational culture through several positions of responsibility.

These case studies highlight some of the differences between corporate reality and academic analysis. Further research is required to determine whether this discrepancy is due to different perceptions or a larger dichotomy between the two. In theory, it is more cost efficient for an organization to meet any possible international standard in one step, but in reality, most chose to only meet the bare minimum required by law at the time a decision became necessary. In most cases, the cost of compliance comprises a base assessment cost and an additional implementation cost and thus it is cheaper for a company (and arguably a country) to meet the highest available standard 'up-front' rather than increasing protection iteratively and incrementally. Economically, it would be more cost effective to meet the highest standard available immediately. Most companies however, cannot justify the additional cost. Indeed, most companies only address legislative reform when it cannot be ignored. For instance, many organisations continue to use and/or store personal information across jurisdictional borders – without any suspicion that they may be in breach of Australian (or other) law.

Most of the businesses surveyed failed to recognise any opportunity costs. One of the major obstacles to international trade is now regulatory. Differing standards of privacy protection pose barriers to trade but most

organizations either trade despite jurisdictional differences or felt they did not apply to them. Research thus far suggests organizations would prefer to either cease transferring personal information across jurisdictional borders or ignore the regulatory requirements of the countries involved until a 'post-hoc' correction is required. Further research would determine whether this approach changes over time as information privacy protection receives greater media attention.

From the legislative trends, it seems clear that an international standard in information privacy protection will emerge over the next few years. The impact of this emerging standard on business varies. Larger organizations and those that trade in numerous jurisdictions will be most affected and likely to apply the necessary due diligence. Large organizations tend to be more aware of legislative requirements and more disposed towards meeting any obligations they may have. Consequently, it is these organizations that have the most to gain from an international standard.

Conversely, smaller organizations tend to either be unaware or ignore legislative requirements that they perceive as irrelevant to their core business interests. Theoretically, these organizations would gain from the strategic adoption of information privacy protections by facilitating cross-jurisdictional trade for little capital outlay. As a smaller organisation, the cost of compliance would be lower and the competitive advantage greater. The reality, however, is that smaller organizations lack the resources (or will) to invest in their long-term future in these areas given the commercial realities of surviving now.

REFERENCES:

Andrews, S. (2002) *Privacy and Human Rights 2002*, Electronic Privacy Information Centre, (last accessed October 2002 at URL http://www.privacy.org/pi/survey/phr2002/)

Australian Attorney General (2001) *European Data Protection Commissioners Opinion of Australia's Privacy Law*, Press Release (last accessed September 2002 at URL www.law.gov.au/aghome/agnews/2001newsag/941_01.htm).

Australian Senate Legal and Constitutional Committee (1999) *Privacy in the Private Sector: Inquiry into Privacy Issues, including the Privacy Amendment Bill 1998*, Commonwealth of Australia (last accessed September 2002 at URL http://www.aph.gov.au/senate/committee/legcon_ctte/privacy/).

Cant, S. (2001) Privacy Worries 'nitpick', *The Age*, August 21.

European Parliament (1995) Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal of the European Communities of 23 November 1995* No L. 281 p. 31

Featherly, K. (2001) *U.S. Cos. Don't Make 'Safe Harbor' Privacy Grade – Study*, Washtech.com (last accessed September 2001 at URL www.newsbytes.com).

Kirby, J. (1996) *Privacy Protection, a new beginning: OECD principles 20 years on*, PLPR (1996) 6(3) 25-29, 27.

Organisation for Economic Development (1980) *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD.

Pedersen, A. (2002) Report reveals serious flaws in Safe Harbor Agreement, Europemedia.net (May 03 at http://www.europemedia.net/shownews.asp?ArticleID=8608)

Reidenberg, J. (2001) *Testimony of Joel R. Reidenberg before the Subcommittee on Commerce*, Trade and Consumer Protection United States House of Representatives (last accessed January 2002 at URL reidenberg.home.sprynete.com).

Slane, B. (2001) *New Zealand's Privacy Law in Perspective*, New Zealand Privacy Commissioner, Proceedings of the LawAsia Conference 2001, Christchurch.

Thibodeau, F. (2001) *Financial Firms Dread California's Tougher Privacy Bill*, Computerworld Online (last accessed February 2002 at URL www.ITworld.com).

COPYRIGHT