The Journal of Contemporary Issues in Business and Government
2007 Volume 13, Number 1, pp 15-30

A French-Australian Comparison of Responsibilities for the Monitoring of Security and Privacy Issues Resulting from the Introduction of New Information Technologies

Lynn M Batten
Deakin University

Gwendal Le Grand
GET/Télécom-Paris

Abstract

Information technologies have altered the way individuals, businesses and societies live and operate. Along with these changes has come loss of privacy and threats to the security of confidential information. Much research in the social sciences has established marked inter-relationships between technology, society and culture. However, the roles of corporations and governments in ensuring maintenance of security and privacy for citizens are unclear. This study determines and compares the roles and responsibilities of stakeholders in both France and Australia in monitoring and responding to security and privacy issues resulting from the introduction of new information technologies. It is found that governments in these countries remain at arm's length from regulation while investing many resources in education of the public and of small business concerning these issues.

Introduction

While many research projects and company and government reports have provided a technical vision of security and privacy (McCarthy & Fonseca, 2003; Riguidel *et al*., 2004; Riguidel *et al*., 2005; Yang, 2005; Le Grand *et al*., 2006) and while research in the social sciences (Waters, 2003; Rose, 2006) has established marked inter-relationships between technology, society and culture, there has been little focus in the literature on where responsibility lies for the impact of digital technologies as they relate to security and privacy. This study breaks new ground in this area.

The right of an individual to reserve some information about him or herself from local or national government scrutiny in not a concept familiar to people in all countries. It

is prevalent in Western Europe, North America, Australia and New Zealand, while in most other parts of the world, one finds little legislation supporting the rights of a citizen to privacy. Securing information has many of the same aspects as retention of privacy of information and so any legislation regarding one tends to impinge on the other. This study, therefore, focuses on those parts of the world where rights to privacy and information security are acknowledged in legislation.

Two countries, France and Australia, were chosen as representatives to provide some insights into the roles of large corporations and government organisations. France and Australia are developed nations with dissimilar histories and cultures, resulting in distinctly different approaches to security and privacy issues and laws by citizens, governments and industries. Both countries have invested heavily in information and communication technology development, yet neither has undertaken in-depth analysis of the impact of security and privacy attitudes on the up-take of these technologies. The research objective of the current study is therefore to:

> *Determine the roles and responsibilities of stakeholders in both France and Australia in monitoring and responding to security and privacy issues resulting from the introduction of new information technologies.*

Initial work on this objective was reported in Batten and Le Grand (2006) and Le Grand and Batten (2006), which comprised responses to a series of interviews with companies selling security and privacy products in both countries. Those interviewed had lengthy experience in their industry setting and were representative of their peers in their industry setting. The key findings of these studies were:

I. Clients are learning more about their need for security and privacy products without knowing technical details.

II. For companies dealing specifically in security products, the selling of security is a challenge. Security is viewed as necessary only when required by regulation or because of liability. The marketing of information security has always been, and continues to be, a problem, though with additional governmental requirements in the last few years it is becoming easier to sell.

III. A potential client will look for an established, reputable organisation from which to purchase security or privacy products.

IV. People are willing to accept a loss of privacy for the sake of convenience.

One of the implications of the last point (IV) linking directly to legislation, or a lack of it, is that major new systems need to be linked to both legislation and policy and that appropriate controls need to be put in place. This is supported by the work of Rose (2006) and is directly related to the research objective.

The current study completes the research objective by reporting on interviews with government and private sector representatives. In section two, the theoretical framework is presented, followed by methodology in section three. Sections four and five contain the results of interviews while sections six and seven analyse and summarise these results.

Related Work and Theoretical Framework

Trust is an issue that is often raised in discussions on privacy and security in technologies. Trust is at the heart of security as its existence, its level and/or features determine the need and relevance of the deployment of security mechanisms, and vice-versa. According to Gambetta (1990: 6), trust:

> *… is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his own action.*

Yang (2005) points out, furthermore, that trust is an important dimension of social capital as it is essential in relationship building. In both France and Australia, studies (Farquharson & Critchley, 2004; Le Grand *et al.*, 2006) have shown that most people are trusting of small business and of public organisations such as hospitals and universities, while they do not trust governments, major companies, trade unions or the media. In a 2003/2004 survey by Farquharson and Critchley (2004), on the attitudes of Australians to new technologies, the authors conclude that:

1. *Australians trust the environmental movement more than they trust governments.*
2. *Trust in government, business and media predict levels of comfort with new technologies.*

In 1998, Alain Weber, President of the Computer and Freedom Commission of the Human Rights League, France, stated that governments should never be trusted concerning the use of new technologies as they use them for more and better surveillance. He goes on to say that citizens are not aware of the dangers of rampant technology development.

Rose's (2006) examination of the concerns around information privacy in New Zealand led her to determine that the greatest concern regarding technology development was for unauthorised access to data. She points out that individual controls are necessary to ensure a normative right to privacy but that these need to be complemented by external controls such as a privacy law. In addition, education of the public about the mechanisms in place is a critical part of the implementation of privacy rights and legislation. This is in line with comments made in the Introduction concerning the last point (IV) linking directly to legislation, or the lack of it, that major new systems need to be linked to both legislation and policy and that appropriate controls need to be put in place.

The work of Milberg, Smith and Burke (2000) classifies countries based on the level of government involvement in corporate privacy management across a range of possibilities from 'self-help', where the individual is responsible for identifying and following through on problems, to a 'licensing' scenario, in which any data bank containing personal data is required to be licensed by a government institution. In explaining these differences about the level of government involvement in corporate privacy management, their study indicates that:

> *A country's cultural values are associated strongly with the privacy concerns exhibited by its populace and are associated marginally with its regulatory approach ... Moreover, if corporations exhibit loose management of information privacy, then individuals are more likely to call for strong privacy laws rather than allowing corporations to self-regulate. Similarly, as individual's privacy concerns rise, so do their demands for legal intervention* (p. 42).

Demands for legal intervention do not always result in the expected response from a government. Determining the response of governments to such demands is a part of the research objective of this study, and so the authors constructed three hypotheses against which to test the information gathered from the literature and their interviews.

Hypothesis 1

Consumers are concerned about security and privacy and so prefer to purchase products with enabled security and privacy mechanisms.

This first hypothesis is based on the aforementioned observation that *Clients are learning more about their need for security and privacy products*. If indeed consumers *are* becoming more aware, are they then seeking out products which incorporate privacy and security mechanisms?

Hypothesis 2

Governments play a supervisory role in ensuring that new technologies have no negative impact on citizens.

Several comments from the literature referred to earlier in this section indicate that consumers do not trust government to protect citizens from untoward hazards resulting from the use of information technologies. Consequently, this hypothesis was developed, which the authors expected would be unsupported.

Hypothesis 3

Cultural differences between Australia and France result in differing attitudes in these countries towards security and privacy.

Finally, in determining differences between the two target countries based on culturally and historically different backgrounds, this third hypothesis was proposed.

Methodology

In order to test Hypothesis 1, the researchers questioned suppliers of security and privacy products about the attitudes and behaviour of their customers. This allowed the research to cover a broad scope of products by selecting companies spanning several sectors, and also to make use of marketing intelligence gathered by the organisations over a period of some years.

The authors compiled a number of questions for use as the basis of interviews with businesses working in the security industry. They identified a number of such organisations in both Australia and France that were representative of the goods and services available in the marketplace to private individuals, enterprises and government

organisations. Chosen for interviews from these were comparable enterprises in Australia and France likely to be affected either in product development or in marketing strategies by security or privacy concerns of their clients. In each case, interviews were held with either the CEO of the organisation or the person with final responsibility for the development and marketing of the goods and services provided. In all cases, discussion was open-ended and the person interviewed was encouraged to add additional relevant information at will. The organisations are listed below but, for confidentiality reasons, interviewees have not been individually identified. The organisations are as follows:

Australia

Biometix, Sydney - A small business providing biometric solutions to a wide range of customers.
EAN Australia, Melbourne - The Australian entity responsible for the supply of bar codes and consequent tracking of information to all Australian businesses.
KeyTrust, Melbourne - A medium-sized company providing trust-based solutions to business and government.
Giesecke & Devrient, Melbourne - A large Australian smart card provider.

France

GENCOD, Paris - The French entity responsible for the supply of bar codes and consequent tracking of information to all French businesses.
Thales Communications, Paris - A large business supplying defence security solutions to governments and large industry.
Wavestorm, Paris - A small organisation providing custom-designed solutions for communications technologies.

Discussions revolved around the product development and marketing phases, being the main areas upon which the customer has the greatest impact. The customer, in the case of those organisations interviewed, is industry or government, and so the results of the discussions with them have repercussions across the entire security sector. Thus, what the interviewee is able to tell us about attitudes of their customers is core to the study's comparison of attitudes towards security and privacy in the two countries and the economic implications of this, and so responds to Hypotheses 1 and 3. A summary of the responses is given in section 4.

In testing Hypothesis 2, the researchers chose not to seek a *perception* of what the government's role was as interpreted perhaps by business, consumers and citizens, but to ask government itself what it felt its role was in ensuring that new technologies have no negative impact on citizens. Consequently, interviews were conducted with government representatives of both Australia and France.

A result of the interviews with companies was a recurrence of the themes of regulation, legislation and policy. With these in mind, the authors then developed a short list of questions, as follows, around which to focus conversations with government and public sector representatives in order to address some of the issues raised. Response II (that security is only implemented when regulation or liability require it) led to the

development of questions about when and why they would regulate security. Response IV (that people are willing to accept a loss of privacy for the sake of convenience) resulted in discussion of legislation, policy and controls, who was responsible for these and when they should be introduced.

Questions for Investigation:

(a) Why do people buy security/privacy in new technology products (marketing and development)?

This question relates to Hypothesis 1.

(b) What role does government play relative to security and privacy issues developing around new technologies?

This question relates to Hypothesis 2.

(c) How does policy and legislation evolve in the context of security and privacy issues developing around new technologies?

This question relates to Hypothesis 2.

(d) What are the critical differences between France and Australia vis-à-vis the above points?

This question was not asked directly, but was an underlying theme in conversations between the authors and participants and relates to Hypothesis 3.

Chosen for interviews were representatives of government organisations with a particular portfolio for information security and privacy concerns. Because of their roles in public office, some of those interviewed asked us to specify them by name and this request was granted. Interviews were also carried out with representatives of several other government agencies and industry bodies who declined to permit us to mention their departments; however, their opinions have been incorporated into the final results and conclusions.

Australia

Paul Chadwick, Privacy Commissioner of Victoria.
Joseph Di Gregorio, a/g GM, Strategy Branch, Information Economy, Department of Communications, Information Technology and the Arts (DCITA), Federal Government.

France

*François Giquel***,** Vice-President of Commission Nationale de l'Iinformatique et des Libertés (CNIL).
M Fort, Head of the Service des Plaintes with CNIL.

Due to the international nature of information technology and the necessity of transmitting it across national boundaries, it was felt to be expedient to interview government organisations of an international nature, closely related to the target countries, which had a mandate for supervising new technologies.

At the international level, two divisions of the Directorate for Science, Technology and Industry of the Organisation for Economic Co-Operation and Development (OECD)

were included as this body has a specific role to play in information communications policy development and encompasses a large number of nations including France and Australia. The OECD is probably the most significant international body with a prescribed role to play in the monitoring of security and privacy in the context of information technology. Those interviewed were:

OECD

Anne Carblanc, Principal Administrator, Information Computer and Communications Policy (ICCP) Division, Directorate for Science, Technology and Industry.
Samuel Paltridge, Economic Analysis and Statistics Division, Directorate for Science, Technology and Industry, OECD.

Results of Discussions with Companies

Outcomes of the discussions with companies in both Australia and France (Batten & Le Grand, 2006; Le Grand & Batten, 2006) are summarised below.

1. All respondents said that customers and clients want security to be built into their goods and services.

2. Some customers and clients want privacy protection to be built into goods and services while others see the lack of privacy as a marketing advantage.

3. Customers and clients do not always understand the costs associated with embedding security and/or privacy protection into goods and services.

4. All respondents said that the attitudes of customers and clients towards security and privacy protection influence the organisation's development decisions.

5. All respondents said that the cost of embedding security and privacy protection into goods and services play a role in the organisation's development decisions.

6. Opinions were mixed on whether security and privacy protection play a role in development plan decision-making.

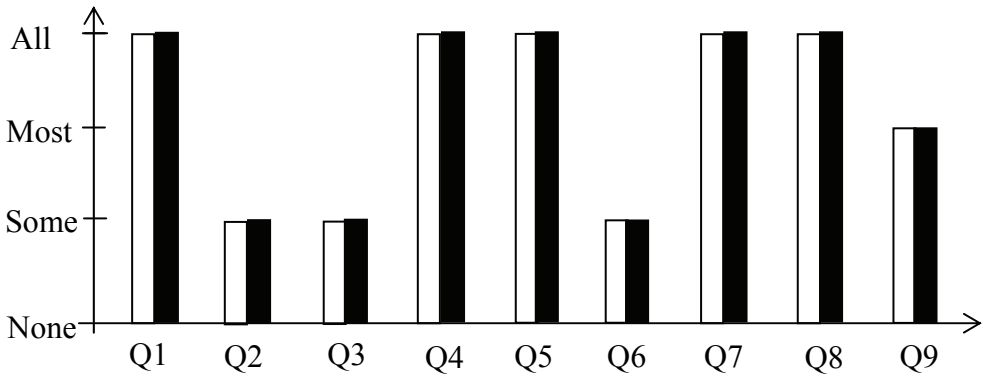
7. All respondents agreed that security is a selling point when marketing the organisation's goods and services.

8. All respondents agreed that privacy is a selling point when marketing the organisation's goods and services.

9. All respondents felt that consumer attitudes towards security will play a role in the marketing of future products.

The responses are displayed graphically (Figure 1) to offer a visual summary of responses to all nine questions, broken into French and Australian opinions.

Figure 1: Summary of Responses from Business



Source: Original table.
Note: Australia □ France ■

Results of Discussions with Government Organisations

While governments of both France and Australia have set up departments to deal with the implementation of information technologies within government and the process of e-business between government and business, they also provide information to non-government organisations on strategies for dealing with information technologies. Alongside these government initiatives, independent bodies have identified needs that cannot be met by government and have become formal organisations to manage these. The authors spoke with representatives of both types of organisations and a selection of their answers are recorded.

On the French Side

In France, interviews were held with La Commission Nationale de l'Informatique et des Libertés (CNIL) in order to understand how France as a nation deals with security and privacy issues around technology. CNIL is an administrative body established in 1978 by laws relating to technology and freedom of the individual. CNIL works independently of government in France, but has formal representation on several high level bodies including parliament and the Senate. CNIL's primary responsibility is the protection of personal data when digital techniques are being used.

Q. Are you monitoring the impact of new technologies?
A: Definitely. For CNIL, the type of data assimilated plays an extraordinarily important role. For instance, biometric data carries an inherent traceability potential. CNIL is not opposed to the use of biometric data for identification, but would argue for complete, secure control of the information by the owner-user. For instance, the information might be on a smart-card held by the user. In case there is a risk of misuse of biometric data, for example, where it was introduced for the purpose of identification and then used for another purpose, such as tracking, CNIL is vehemently opposed.

In this regard, a major impending risk seen by CNIL is the proliferation of databases which are interconnected and for which data correlation is possible.

Q. Whose responsibility is it to educate on privacy and security issues?
A: In addition to their counselling role, CNIL provides a complaint service to citizens enabling them to determine if specific documents are respecting the laws on technology and freedom. CNIL can equally exercise their power of control of sensitive databases such as files regarding claimed infractions by the national police.

Q. What is the impact on policy and legislation?
A: CNIL does not strictly speaking initiate legal projects, but it is consulted on every project related to the protection of the individual when this is connected with automated data handling. In this case, CNIL will provide an opinion which will be taken into account in the discussion or in parliamentary debate. CNIL has several levels of sanctions at its disposal, including warnings and financial penalties, and can influence a court based on its power of persuasion and moral influence. The potential impact on the public image of a business often plays a far greater role in the outcome than the implementation of sanctions.

On the Australian Side

In Australia, interviews were arranged with relevant players at the state level (Victorian) and at the national level. Australia has a Commonwealth Privacy Commissioner mandated to oversee immigration, tax and welfare in the Commonwealth public sector. The federal commissioner deals with the corporate sector, while state privacy commissioners do not. The Office of the federal Privacy Commissioner, created in 1989, is independent of government but has responsibilities under the federal *Privacy Act 1988*. The Jurisdiction of the Privacy Commissioner of Victoria is limited to state and local government. Australia has introduced state level offices of privacy commissioners over the last few years.

Several departments at the federal level, such as DCITA and the Australian Government Information Management Office (AGIMO), have responsibility for the information technologies area and associated concerns such as security and privacy. These departments work with organisations in other countries as well as transnational ones such as the OECD, and with national groups and state governments to develop compatible approaches to dealing with the issues.

Most Australian states have established the position of Chief Information Officer as well as Privacy Commissioner. At the national level, the role of the Chief Information Officer for AGIMO is to foster the efficient and effective use of Information and Communication Technologies (ICT) by Australian Government departments and agencies. AGIMO also works with governments and other bodies at the local, state, national and international levels. The federal government has strong mandates for security in such areas as foreign affairs, messaging and data centres. Its Department of Defence (2006) has developed an extensive manual delineating appropriate communication security practices internal to the federal government.

Q. Are you monitoring the impact of new technologies?
A: DCITA has responsibilities in policy development for key agencies, standards, e-payments, e-research agendas, venture capitals and benchmarking research. It does international work with the OECD in developing risk assessment methodologies, and identifying new markets and services, determining who the providers are and how consumers engage.

The brief of a Privacy Commissioner is to regulate government. Governments always try to invade privacy because governments believe they have:

- *the mandate to survey*
- *legitimate reasons to gather personal data (taxation, maintenance of borders).*

Governments are good customers for people who sell privacy-invasive technologies; they can impose surveillance by law and can determine the degree of their accountability. The Privacy Commissioner's job is partly to explain authorised compromises between competing interests – for example, privacy versus surveillance. Transparency in the handling of information is required and is a constant bargain between the citizen and the State. The government needs to be transparent about collection, purpose and use of data.

Privacy is well covered at the national level through the Privacy Act. However, governments have moved closer to the security than to the privacy end of the spectrum, especially since 9/11/2001. Nevertheless, citizens tend to trust that technology will not be misused and the new generation seems to have higher thresholds for privacy issues because of their familiarity with technologies.

Q. Whose responsibility is it to educate on privacy and security issues?
A: The core role of DCITA is information awareness. Greater skills, better data management and an understanding of secure networks are needed by consumers. Governments should raise awareness universally but it is also the role of large players such as banks, internet service providers and consumers as e-health and e-education become more and more prevalent. It is a key societal issue. DCITA weighs legislation against education and takes the latter road. Its role is to educate government, large business, small and medium business, and the consumer.

Two levels can be distinguished: the home which is uncontrolled and the government which can be controlled. Education is also the responsibility of the home and then of the education system. Privacy commissioners have a role. We are in an age comparable to the industrial revolution when safe practices in the workplace were unknown and developed slowly over time. We have to develop safe practices for the information age. Elected representatives as much as appointed officials have a duty to take a greater interest and to generate deep public discussion. Currently, such discussions are at a primitive level.

Q. What is the impact on policy and legislation?
A: Most of the problems encountered are procedural problems, therefore there is an urgent need to improve policy and this is why the Law Enforcement Assistance Program system examines privacy exposures at the State level. The Australian national Audit Office report contains information on security and privacy around federal government agencies. The Australian Government Information and Communications Technology Security Manual, developed by the Defence Signals Directorate [DSD], *provides policies and guidance to Australian Government agencies on how to protect their ICT systems. The federal government has stronger mandates around security. It has heavy mandates for instance in foreign affairs, messaging and*

data centres. Decentralisation to the States has resulted in fragmentation of regulation and a lack of standards.

The International Perspective

The OECD is an economic intergovernmental organisation which encompasses 30 member countries. NGOs, civil society representatives and official representations of business and industry are also involved in the organisation's work. The OECD also collaborates with international organisations and agencies such as the Council of Europe, the European Union (EU) and the European Network and Information Security Agency (ENISA) on awareness raising and other security issues. Among other tasks, the OECD develops non-binding guidelines and raises awareness in areas where an international consensus agreement is needed; the OECD cannot, however, legislate.

Anne Carblanc heads the OECD Working Party on Information Security and Privacy (WPISP), which develops policy options to sustain trust, information security and privacy in the global networked society. The policies WPISP define are intended to be technology-neutral. With respect to security, WPISP has developed guidelines on the security of information systems and networks in 2002. The Guidelines have been recognised and endorsed by the United Nations (UN), Asia-Pacific Economic Cooperation (APEC), the EU, and Asia-Europe Meeting (ASEM). Subsequent to the implementation of the Guidelines, WPISP released a report in 2005 called *The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries* which details the main characteristics of national policies and strategies for the security of information systems and networks in a number of OECD countries. The objective is to foster the implementation of coherent and coordinated policies to alleviate the absence of national borders online.

Q: Are you monitoring the impact of new technologies?
A: Yes. However, we do this periodically rather than systematically. For instance, WPISP has been active in the fields of biometry, RFID (radio frequency identification) and sensor technologies, cryptography and trust in the online environment.

Q: In your view, whose responsibility is the monitoring of such technologies and where should changes to legislation and regulation originate?
A: WPISP's mandate is to monitor and analyse developments and trends in, and to develop and propose policy options for, the security of information systems and networks, and protection of personal data and privacy in the information society. In this context, WPISP can monitor technologies but changes to legislation and regulation originate from OECD member countries. The OECD itself cannot legislate.

Q: Are citizens ready to give up privacy in return for convenience/security?
A: WPISP focuses on new threats propagated by the Internet and policies to address these threats. Threats include malware, spam, identity theft, privacy breaches. New vulnerabilities are cropping up with new information technologies due to generalized interconnectivity and dynamic availability. WPISP develops policies to address the risks that foster education of all actors, examine economic disincentives and the whole variety of governmental measures, including cross-border law enforcement cooperation.

Q: Whose responsibility is it to educate on privacy issues and contribute to raise awareness?
A: It is the responsibility of governments, businesses, and consumer associations. They must promote security and privacy and raise the public's technical skills by supporting a culture of security and of privacy.

Q: Does the OECD provide some kind of certification for governments or companies when they meet certain standards?
A: The OECD is neutral; it would not recommend a specific tool or technology but it might issue recommendations as to the goals to be reached by businesses or governments in a specific field.

In 2002, the OECD published guidelines for the security of information systems and networks called 'Towards a Culture of Security'. This culture of security was defined as 'a focus on security in the development of information systems and networks and the adoption of new ways of thinking and behaving by all participants when using information systems and communicating or transacting across networks'. The document goes on to list three items which are viewed by the OECD as being part of government responsibility in this domain: awareness raising, the provision of education and training, the provision of information resources to the public.

Analysis of the Discussions as they Relate to the Hypotheses

Hypothesis 1

There was little support for this hypothesis. The opinion was that people do not see added value or functionality from security. Liability, as indicated through a risk management analysis, may be a driver, but such analysis is rarely undertaken. The need for security is acknowledged if the cost of insecurity becomes too high; this cost includes the introduction and management of new security technologies, which is often viewed as being complex. Thus, any such additional functionality merely adds complexity to the product which is not appreciated by the client. Customers look for suppliers with a good reputation as they need to trust them. In addition, they are more comfortable with products that have been on the market for a while rather than with new ones.

Hypothesis 2

There was mixed response to this. While governments felt a responsibility for the impact of new information technologies, they chose education over regulation in Australia. The French system, especially when examining the role of CNIL, seems oriented toward regulation. In general, however, both countries tend to be re-active rather than pro-active, waiting until a technology has found wide adoption and specific problems have been identified before responding.

Governments try to educate and assist citizens and small and medium businesses. However, their relationship with large organisations is different. Government may be independent of large business, as in the banking sector, or dependent on it, as in the ISP and Telco sector. In either of these latter situations, government provides regulatory advice and sometimes enacts legislation about the behaviour of large business. Justice must interpret and enact these laws. When the laws can clearly be executed within a jurisdiction,

this is fairly straightforward, but when they must be interpreted across international boundaries, justice may have little recourse. Faced with the complexity of these issues across international borders, an organisation such as the OECD works towards a consensus but expects the market to be regulated by the big corporate players.

Hypothesis 3

In the spectrum of regulation models used by Milberg *et al.* (2000), both countries appear in the higher end of the scale with Australia placed in the data commissioner model and France appearing one step higher in regulation with the registration model. There is clear evidence that cultural attitudes have placed the two countries in these respective positions; however, with respect to the spectrum offered by Milberg *et al.* (2000), they appear side by side and so in most ways are not far apart.

In Australia, the data commissioner has no powers of regulation, but relies on complaints to initiate process and sanctions. The commissioner is viewed as an expert who should offer advice and monitor operations. The registration model, used in France, requires registration of data banks by a separate, yet government-related entity. This entity has no power to deny registration, but can deregister when complaints are proved to be founded.

Both France and Australia support the OECD guidelines on creating a culture of security. Formal responses were issued by the Secretary General of National Defence in France and by the Attorney-General's Department in Australia. Both countries formalised ties with their respective computer emergency response teams; developed guides on risk evaluation and information dissemination; and developed websites targeting various sectors of the population in order to provide them with pertinent information. Differences between the two countries relative to the OECD guidelines are small. France established a formal training program, with some sessions up to two years in duration, for government staff who are deemed to need such knowledge while Australia has not set up such a formal system. Australia has tended to target small and medium business in constructing informational websites while France has targeted the general public.

Summary and Recommendations

In examining both the corporate point of view and the policy perspective on the roles and responsibilities of stakeholders in both France and Australia in monitoring and responding to security and privacy issues resulting from the introduction of new information technologies, a difference of opinion between the corporate and the government organisations can be seen. On the one hand, corporations have identified a need for regulation by governments in the area in order to ensure an uptake by the consumer of technologies which support privacy and security mechanisms. Their analysis identifies a feeble market for products with such mechanisms unless these are required by law or liability. On the other hand, governments in both countries under analysis have chosen a non-regulatory approach, preferring to develop educational programmes for the purposes of educating the consumer as to why they need to be aware of information security and privacy issues.

There was no support for Hypothesis 1. Indeed, corporate business indicated that consumers were loath to purchase security and privacy components which appeared to add no value to the product. There was partial support for Hypothesis 2. Government organisations are certainly aware of the issues and ready and willing to supply informative material; however, they are not ready to introduce legislation forcing suppliers to build in the necessary mechanisms, nor consumers to purchase them. There was also partial support for Hypothesis 3. At the corporate level, there is clearly no difference in attitude or in experience of the market issues between Australia and France. At the government level, there are differences in the regulation models chosen by the two countries.

In Agre and Rotenberg (1997: 6), the authors state that: 'Privacy issues have begun to arise in more various and more intimate ways, a greater range of design and policy options are available, and some decisions must therefore be made that are both fundamental and extraordinarily complicated'. This study supports this view by showing that governments have increasing opportunities to use technical means both for protecting privacy and for invading it. Governments have an opportunity to educate individuals as to the means at their disposal to control access to information about themselves. However, a more fundamental approach would be for governments to ensure that they themselves do not have the ability to abuse their own access to data about individuals. This study shows that this is not a path governments will be following.

On the other hand, given the pressure to develop an international approach, the following comment of Milberg *et al.* (2000, p. 53) is to be considered:

> *Consumers and legislators in different societies will exhibit varying levels of concern about information privacy, both in general and in their assessment of specific practices. Thus a universal regulatory approach to information privacy seems unlikely and would ignore cultural and societal differences.*

The outcomes of this study do not necessarily support this comment. The OECD has shown itself to be a powerful factor in rationalising approaches to security and privacy concerns while allowing space for individuality of approaches. Their 'culture of security' document details the main characteristics of national policies and strategies for the security of information systems and networks in OECD countries.

The authors believe that over time, an international perspective and extensive collaboration in dealing with information security and privacy issues on the part of government will be possible. What role governments play in this remains to be seen, but it is clear from this research that education rather than legislation will be their general approach.

Acknowledgements

The authors wish to thank Forum for European-Australian Science and Technology Cooperation (FEAST) for providing financial support for this research.

References

Agre, P.E. and Rotenberg, M. (1997) *Technology and Privacy: The New Landscape*. MIT Press, Cambridge, MA.

Attorney-General, Australian Government (2003) *Implementing a 'Culture of Security' in Australia*. Australian Government. (Available from: http://www.oecd.org/dataoecd/18/21/36290761.pdf.)

Batten, L.M. and Le Grand, G. (2006) A French-Australian comparison of attitudes towards security and privacy modern information technologies. *Proceedings of the Internet Society II. Proc. Int. Symp*, Wessex, pp 415-424.

Defence Signals Directorate (2006) *Australian Government Information and Communications Technology Security Manual* (September). Australian Government. (Available from: http://www.dsd.gov.au/library/infosec/acsi33.html.)

Farquharson, K. and Critchley, C. (2004) Risk, trust and cutting edge technologies: A study of Australian attitudes. *Australian Journal of Emerging Technologies and Society*, 2 (2) pp 1-23.

Gambetta, D. (1990) *Can We Trust Trust?* Basil Blackwell, New York, NY.

Le Grand, G. and Batten, L.M. (2006) Government responsibilities for the monitoring of security and privacy issues around new information technologies: A French-Australian comparison. Recent advances in security technology. *Proceedings of the 2006 RNSA Security Technology Conference*, Canberra, pp 181-191.

Le Grand, G., Riguidel, M., Urien, P., Serhrouchni, A., Tchepnda, C., Naqvi, S., Tastet, F., Lopez, G., Johnson, J., Arujo, J., Gessler, G. and Feroul, M. (2006) Final trust, security and policy framework (Report), Sixth Framework Programme Priority 2, Security Expert Initiative.

McCarthy, J. and Fonseca, B. (2003) Trusting ID management technology. *Information Age*, Aug/Sept pp 35-39.

Milberg, S.J., Smith, H.J. and Burke, S.J. (2000) Information privacy: Corporate management and national regulation. *Organization Science*, 11 (1) pp 35-57.

OECD Directorate for Science, Technology and Industry, Working Party for Information Security and Privacy (2003) The promotion of a culture of security for information systems and networks in OECD countries. (Available from: http://www.oecd.org/dataoecd/16/27/35884541.pdf.)

Premier Ministre, Republique Française (2004) *Cahier des Clauses Techniques Particulieres*, 16 April 2004. (Available from: http://www.ssi.gouv.fr/fr/actualites/marches/traduction/CCTP_n2004-04_du_16-04-04.pdf.)

Riguidel, M., Urien, P., Serhrouchni, A., Le Grand, G. and Naqvi, S. (2004) *Assessment of Threats and Vulnerabilities for Networks*. Sixth Framework Programme Priority 2, Security Expert Initiative. August.

Riguidel, M., Urien, P., Serhrouchni, A., Le Grand, G., Chiollaz, C., Naqvi, S., Skarmeta, A., Johnson, J., Araujo, J. and Roth, M. (2005) *Policy Framework Models and Interrelation* (Report), Sixth Framework Programme Priority 2, Security Expert Initiative. February.

Rose, E.A. (2006) An examination of the concern for information privacy in the New Zealand regulatory context. *Information & Management*, 43 pp 322-335.

Waters, N. (2003) The European influence on privacy law and practice. *Proceedings of Conference on International Dimensions of E-commerce and Cyberspace Regulation,* Sydney, pp 150-155.

Weber, A. (1998) Presentation to workshop Surfiches, ne vous en fichez plus, Paris, 25 April. (Available from: www.delis.sgdg.org/menu/25avril/2504aw.htm.)

Yang, S. (2005) Relationships among mobile data service, mobility and the social capital: A conceptual model. *Proceedings of the 16th Australasian Conference on Information Systems*, December, pp 82-90.