# A French-Australian comparison of attitudes towards security and privacy in modern information technologies

L. M. Batten[1] & G. LeGrand[2]
[1]*Deakin University, Melbourne, Australia*
[2]*GET/Télécom-Paris (ENST), LTCI-UMR 541 CNRS, France*

## Abstract

The purpose of this research is to analyse social response, both at the individual and the corporate level, to the security and privacy concerns raised by new technology development, with particular reference to comparisons in attitudes between Australia and France. Interviews were conducted with three organizations in each country, all of which provide goods and services which protect and manage data. Four of the organizations operate at international or national levels and have been in existence for many years. Two were small companies which had been in existence for only a few years.

Across both countries, our interviews indicated that security is not an item that people are willing to pay for unless it is required by law or deemed necessary, for instance, in order to obtain insurance benefits. However, one interviewee noted that both citizens and organizations are becoming more educated about what security means and what it does, and this will eventually lead to an increase in demand for privacy and security products.

The most distinctive difference in attitudes between France and Australia were found in the privacy area, Europe and France having a far more stringent legal approach to the protection of privacy than Australia. The specific disparities arise around categories of exemptions, the existence of legally authorized 'privacy violations' in Australia, the handling of sensitive data, and the length of time for which data should be kept confidential.

*Keywords: information privacy, data security, culture.*

WIT Transactions on Information and Communication Technologies, Vol 36, © 2006 WIT Press
www.witpress.com, ISSN 1743-3517 (on-line)
doi:10.2495/IS060391

## 1 Introduction

Information technologies have altered the way individuals, businesses and societies live and operate. Increased speed, greater access, extended flexibility have all been outcomes of the latest technological developments [13]. Hand in hand with these changes have appeared a loss of privacy along with threats to the security of confidential information [12]. While new technology is marketed internationally and available relatively easily in any country, privacy and security vary from culture to culture as they are often tied to the tradition of the place and the restrictions brought to bear by the governing bodies. This situation raises the following question: to what extent do cultural attitudes towards privacy and security affect the take-up and use of new information technologies?

In this context, the objectives of the current work are to determine the key points of difference and of similarity in such attitudes in two geographically quite distinct parts of the world. France and Australia are developed nations with different histories and cultures, resulting in distinct approaches to security and privacy issues and laws by citizens, governments and industries. Both countries have invested heavily in information and communication technology development. However, neither country has undertaken an in-depth analysis of the impact of security and privacy attitudes on the up-take of these technologies.

The research objectives of the current work are therefore to fill this gap by:

*1. Analysis of the impact of security and privacy attitudes on the up-take of information and communication technologies in each of Australia and France independently.*

2. *Comparative analysis of the key points of difference and of similarity in attitudes towards security and privacy in France and Australia by individuals, small, medium and large corporations and governments.*

While many research projects, company and government reports have provided a technical vision of security and privacy [9, 11, 16], they have rarely taken into account the social aspects and impacts of digital technologies as they relate to security and privacy, thus the current work breaks new ground in this area.

In subsequent sections of the paper, we outline our methodology, discuss the relevant literature, describe the interviews, results and implications, and summarize our work.

## 2 Methodology

As background to the research, a thorough survey of relevant literature on social response, both at the individual and the corporate level, to the security and privacy concerns raised by new technology development was undertaken. A summary of this appears in section 3. Subsequently, the authors compiled a number of questions for use as the basis of interviews with small, medium and large businesses working in the security industry and identified a number of such organizations in both Australia and France which were representative of the goods and services available in the marketplace to private individuals, enterprises and government organizations. Chosen for interviews from these were comparable enterprises in Australia and France who are 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 organization or the person with final responsibility for the development and marketing of the goods and services provided. For confidentiality reasons, we list the organizations below but do not identify the individual with whom we spoke.

The organizations were 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.

**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 organization providing custom-designed solutions for communications technologies.

Discussions revolved around the product development and marketing phases of the operation, as these are the key areas upon which the customer has the most impact. For the most part, these businesses supply to other organizations, either in industry or government, and so the results of the discussions with them are core to our comparison of attitudes towards security and privacy in the two countries and the economic implications.

Our analysis around individuals is based mainly on the research literature as it was not possible, with the resources available, to survey large numbers of people.

## 3 Social implications

'It is now widely accepted in the social sciences that there is an inter-relationship between technology, society and culture. Users shape the technologies as much as they are shaped by them. However, much of the policy and technological discussion continues to have the flavour of a one-way relationship – that of the impact of technology on society.' [5].

On the other hand, consumer response to new technologies is certainly the deciding factor in whether a new product will remain on the market for a significant period of time. While mobile phones have changed the way people communicate and SMS text messaging has affected the languages with which they communicate, these changes in behaviour would not have occurred if the individuals purchasing the products had not been ready to embrace and adapt to the new technology. As noted by Lacohee et al. [7] –'Text messaging may have been created by engineers, but its take-up was still surprising to most (a text-messaging-phone invention in 1991 was dismissed as irrelevant by senior BT managers – why would anyone want to send text when they can talk to someone?)'.

Why do some new technologies find large markets and others not? The example of the mobile telephone is an interesting one which has been studied in many countries. Anderson et al. [2] and Anderson and Tracey [3] in the European context argue that mobile phones are a major source of the development of social relationships and networks. Agar [1] goes further, pointing out that the mobile telephone has been '…a way of rebuilding economies in eastern Europe, an instrument of unification in western Europe, a fashion statement in Finland or Japan, a mundane means of communication in the USA…an agent of political change in the Philippines.' In the Australian context, Yang [15] agrees that 'social capital', the value of social networks, constitutes a valuable resource provided by mobile phone technology.

Trust is an issue that is often raised in discussions of privacy and security issues in technologies. Yang [15] points out that trust is an important dimension of social capital as it is essential in relationship building. In both France and Australia, studies [6, 8] have shown that most people are trusting of small business and of public organizations such as hospitals and universities. They do not trust governments, major companies, trade unions or the media.

In a 2003/2004 survey [6] of the attitudes of Australians to new technologies, Farquharson and Critchley conclude that:

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

In 1998, Alain Weber, President of the Computer and Freedom Commission of the Human Rights League, France, stated [19] that governments should never be trusted concerning the use of new technologies, which are always used by them for more and better surveillance. He goes on to say that citizens are not aware of the dangers of rampant technology development. Moreover, several organizations such as Fédération Informatique et Libertés [18] condemn the intrusion of governments in daily life and try to preserve the privacy the citizen obtained with the 1978 law on computing and freedom (informatique et libertés), which later inspired work of the European Commission. Despite the fact that changes to this law must be approved by the Commission Nationale

Informatique et Libertés, and are lengthy and difficult, by 2004 we see a marked diminution of the privacy rights of French citizens.

## 4 Results of the interviews

In this section, we present the views of the organisations involved in interviews. The two areas of discussion were product development and marketing, and within each of these were several questions. Below, A stands for Australia and F for France.

### 4.1 Product development

1. ***Do you believe that your customers and clients want security to be built in to your goods and services? Percentage of customers/clients? For what reasons or purposes?***

A: All respondents said yes, all clients expect this. Export business was listed as one key reason. It was noted that over the last five years there has been a marked change in attitude towards sales of communications security goods and services since clients are becoming more familiar with the issues. When people recognize the need for security and also recognize that they cannot implement it themselves, then they are willing to pay for it. There is little government or other regulation mandating it.

F: All respondents said yes, all clients expect this, while one organization (GENCOD) said that this referred to reliability rather than security. Clients have insufficient knowledge of security products and so rely on a well established reputation in the area. For some clients, certain security levels are regulated; for others, liability is the incentive.

2. ***Do you believe that your customers and clients want privacy protection to be built in to your goods and services? Percentage of customers/clients? For what reasons or purposes?***

A: All respondents felt that their clients had mixed answers here. EAN said that some clients see lack of privacy as a marketing advantage. Other comments distinguished between governments, viewed as seeking privacy, and business, viewed as seeking security. The development of privacy law, policies and procedures is viewed as being the job of the larger community and not just government.

F: GENCOD felt that the fact that all its data is made publicly available belies the need for privacy altogether. The other responses were also in the negative, except that Wavestorm stated that its clients want data privacy but not location privacy.

3. ***Do you believe that your customers and clients understand the costs associated with embedding security and/or privacy protection into your goods and services?***

A: Responses were very mixed ranging from off-setting price against liability to the idea that security and privacy costs are hidden costs.

F: Most such costs are hidden from the clients and so they neither see nor understand them.

4. ***Do the attitudes of your customers and clients towards security and privacy protection influence the organization's development decisions? In what ways? How strongly?***

A: Each response was in the affirmative. KeyTrust pointed out that they sell trust because that is what clients will pay for. All said that they designed product security and privacy for the needs of the client.

F: All respondents were affirmative with Wavestorm feeling that clients want simplified systems which results in lower levels of security. Thales pointed out that selling security can be difficult as it is often reactive - clients will often look for a trusted organization from which to purchase security products.

5. ***Does the cost of embedding security and privacy protection into goods and services play a role in the organization's development decisions? How? To what extent?***

A: KeyTrust responds to this issue by having low-cost entry points and trading security for liability. EAN pointed out that audits have associated costs.

F: Responses were mixed, with GENCOD saying no and the others saying yes. Thales gave an explicit figure of security costing about 20% of the initial product evaluation.

6. ***Do security and privacy protection play a role in development plan decision-making?***

A: EAN said none whatever; Biometix said their products are security products and so the answer is yes. KeyTrust said that there was a need for an independent privacy and identity organization in Australia.

F: GENCOD said no; Wavestorm yes, but in the sense of their response to question 5; Thales said yes, and was concerned that re-selling of their products to others would entail loss of guarantees of built-in privacy and security.

### 4.2 Marketing

***1. When marketing your organization's goods and services, is security a selling point?***

A: All respondents agreed that it was.

F: All respondents replied in the affirmative.

***2. When marketing your organization's goods and services, is privacy protection a selling point?***

A: Replies were affirmative, but weaker than for security.

F: Responses were varied. GENCOD sees reliability as a marketing strategy.

***3. Do you see consumer attitudes towards security playing a role in the marketing of future products?***

A: Respondents identified convenience and personalisation as marketing opportunity responses to consumer attitudes.

F: Reliable data was viewed as being important. Regulated security might be considered in some sense a consumer attitude.

There are no significant differences, based on nationality, between the responses above. Some interesting points about attitudes to security and privacy which are worth noting come out of the discussion:

**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 deemed so because of regulation or 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 organization from which to purchase security or privacy products.

**IV.** People are willing to accept a loss of privacy for the sake of convenience. Therefore, major new systems need to be linked to both legislation and policy and appropriate controls put in place.

With respect to point IV, it was noted by one interviewee that in Europe, people have carried mandated identification for many years, while this is not the case in Australia. The former situation leads slowly to an acceptance of lower levels of privacy.

## 5 Governance

New technology comes with associated risks, but the real risks are unknown because the technology is new. Governments and organisations tend to manage such risk by means of regulation. Farquharson and Critchley [6] conclude that 'Trust in the institutions behind new technologies therefore seems important for people living in a risk society like ours. For people to be comfortable with new, cutting edge technologies, trust in these institutions is an important precursor. If governments and/or private businesses want people to be comfortable with their technologies, arranging their development through trustworthy groups (such as public science) and transparent processes would be a promising strategy.' In Australia, France and many other countries, governments and large organizations have made considerable efforts to encourage small and medium enterprises to engage in electronic trading. Despite these efforts, such businesses have been slow to adopt new electronic business-to-business trading at anything more than a superficial level [4], confirming the lack of trust mentioned in section 3.

One of the ways that Australia has attempted to develop an atmosphere of trust is by the establishment of the office of the Australian Federal Privacy Commissioner. In [10], this office defines ten basic principles regarding Information Privacy on its site, eight of which relate to electronic information privacy.

The European Union also addresses privacy principles in the EU Data Protection Directive 95/46/EC [17]. Articles 25 and 26 address data protection and privacy issues, and in particular, deal with the transfer of personal information to countries outside of the EU. Article 25 deals with the transfer of personal data to (third world) countries where there is adequate protection of personal data in the intended country. The term 'adequate' is pivotal in this context; it is interesting to note the profound changes to the 1978 law as a result of the later directive.

Interestingly, there are claims [14] that Australia fails the 'adequacy' definition in its privacy laws, thus highlighting discrepancies between Australia and the EU. These discrepancies include exemptions, legally authorized 'privacy violations', the handling of sensitive data, and the length of time for which data should be kept confidential. This appears to be the only significant area within the scope of this research where France and Australia are in disagreement, and may be related to the fact that France has had national level government mandated groups responsible for the oversight of data privacy for about twenty years longer than Australia.

## 6 Conclusions and further work

The security of the digital world has become a fundamental objective of the citizen with respect to individual freedom and protection of privacy and computerized identity and of the corporation with respect to the protection of computerized assets, business transactions and the reliability of its information networks. For the state, digital network security means reliability of operations and reduction in the vulnerability of large and critical infrastructures such as electricity and water distribution systems, and communication and information systems relating to these.

Both France and Australia have invested heavily in information and communication technology development while neither country has undertaken an in-depth analysis of the impact of security and privacy attitudes on the up-take of these technologies. The current work begins to fill this gap.

The findings of this research will subsequently be presented to government and legal experts for information on their understanding of the political and legislative implications. This will enable us to investigate implications for the economies and legislation at national and international level for both countries as well as the impact on international law.

## References

[1] Agar, J., Constant Touch: A Global History of the Mobile Phone. Icon Books, Cambridge, 2003.

[2] Anderson, B., Gale, C., Gower, A. P., France, E. F., Jones, M. L. R., Lacohee, H. L., McWilliam, A., Tracey, K. and Trimby, M. Digital living – people-centred innovation and strategy. BT Technology Journal, 20(2), pp. 11-29, 2002.

[3] Anderson, B. and Tracey, K., Digital living: The impact (or otherwise) of the Internet on everyday life. The Internet in Everyday Life, eds. B. Wellman and C. Haythornwaite, Blackwells: Oxford, 2002.

[4] Batten, L.M. and Castleman, T., Securing small business – The role of information technology policy. Proc. of the 16th Australasian Conference on Information Systems, December 2005.

[5] Beaton, B. and Wajcman, J., The impact of the mobile telephone in Australia. Proc. of Conference of the Australian Mobile Telecommunications Association Conference, 27 pp., Sept. 2004.

[6] Farquharson, K. and Critchley, C., Risk, trust and cutting edge technologies: A study of Australian attitudes. Australian Journal of Emerging Technologies and Society, vol 2, no. 2 2004 pp. 1-23.

[7] Lacohee, H., Wakeford, N. and Pearson, I. A social history of the mobile telephone with a view to its future. BT Technology Journal, 21(3) 2003.

[8] 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.. Final Trust, Security and Policy Framework. Sixth Framework Programme Priority 2, Security Expert Initiative, December 2005.

[9] McCarthy, J. and Fonseca, B., Trusting ID Management Technology. Information Age, pp. 35-39, Aug/Sept 2003.

[10] Office of the Privacy Commissioner, 2004, "National Privacy Principles" Extract from the Privacy Amendment Act 2000. See www.privacy.gov.au.

[11] Riguidel, M., Urien, P., Serhrouchni, A., Le Grand, G., Chiollaz, C., Naqvi, S., Skarmeta, A., Johnson, J., Araujo, J. and Roth, M. Policy framework models and interrelation. Sixth Framework Programme Priority 2, Security Expert Initiative. February 2005. Available at http://www.seinit.org/documents/Deliverables/SEINIT_D1.3_Public.pdf.

[12] Riguidel, M., Urien, P., Serhrouchni, A., Le Grand, G., Naqvi, S., Assessment of threats and vulnerabilities for networks. Sixth Framework Programme Priority 2, Security Expert Initiative. August 2004. Available at www.seinit.org/documents/Deliverables/SEINIT_D1.2_PU.pdf

[13] Ubiquitous Network Societies: The Case of Japan. Proc of ITU workshop on Ubiquitous Network Societies, April 2005.

[14] Waters, N., The European influence on privacy law and practice. Proceedings of a Conference on International Dimensions of E-commerce and Cyberspace Regulation, Sydney 2002. Published by Australian Law Journals Project. 2003

[15] Yang, S., Relationships among mobile data service, mobility and the social capital: a conceptual model. Proc. of the 16th Australasian Conference on Information Systems, December 2005.

[16] Cordis,www.cordis.lu/france/programmes_c1.htm

[17] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, www.cdt.org/privacy/eudirective/EU_Directive_.html

[18] Fédération Informatique et Libertés, http://www.vie-privee.org

[19] Weber, www.delis.sgdg.org/menu/25avril/2504aw.htm