This is the published version:


Available from Deakin Research Online:

http://hdl.handle.net/10536/DRO/DU:30009742

Reproduced with the kind permission of the copyright owner.

Government responsibilities for the monitoring of security and privacy issues around new information technologies - a French-Australian comparison

Gwendal LeGrand
GET/Télécom-Paris (ENST), LTCI-UMR 541 CNRS, France

Lynn M. Batten
Deakin University, Melbourne, Australia

Abstract
The purpose of this research is to determine the understanding of government organizations as to their role regarding 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 individuals from government or public sector organizations in each country with responsibilities for understanding the security and privacy issues as they relate to citizens. Findings of this work should have implications for national and international policy.

Biographies
Dr. Gwendal LeGrand has worked as an Associate Professor in the Computer Science and Network Department of Ecole Nationale Supérieure des Télécommunications since 2001. He received his PhD in computer science from the University of Paris 6 in July 2001 and graduated as a telecommunications engineer of the Institut National des Télécommunications in Evry, France in 1997. His main research interests are oriented
towards wireless and ad hoc networking, security of information systems, communication protocols and quality of service. He is involved in several national and European projects in computer networking, security and security of critical infrastructures.

Lynn Batten is Director of the Information Security Research Group and Professor of Mathematics at Deakin University. Prior to this, she was Head of the Department of Mathematics, and then Associate Dean, Academic and Industrial Research, at the University of Manitoba in Canada. Her current research includes areas within the framework of information security including policy and regulation, business uses, public key infrastructures, wireless security, computer forensics and cryptographic protocols. Professor Batten has organized a number of security conferences in Melbourne in the past five years, and has served as member of the program committee of numerous international security conferences.

Introduction

While new technology is marketed internationally and available relatively easily in any country, privacy and security concerns 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 to assist in filling this gap by:

Determining the key points of difference and of similarity in the roles played by governments and public sector organizations in France and Australia in the development of policy dealing with security and privacy concerns raised by new technology developments.

While many research projects, company and government reports have provided a technical vision of security and privacy (McCarthy & Fonseca 2003, Riguidel et al. 2005, Cordis 2006), 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. Initial work on these objectives was reported in (Batten
Recent advances in security technology

& LeGrand 2006). One of the key findings from that study, which comprised a series of interviews with companies selling security and privacy products in both countries, was:

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

The companies producing the technologies sometimes realize the implications for security and privacy that these technologies hold, yet they are driven by commercial ends and are not obliged by law to inform the customer of the impact of the technology uptake. The above recommendation would encourage the involvement of government in determining appropriate policy around such technologies.

In order to follow up on this issue, the authors approached several government, national and international organizations with responsibilities for policy and legislation to determine their view of their responsibilities in influencing or introducing regulation. In the current paper, we report on discussions with these organizations, both in France and in Australia, and summarize our findings in the conclusion.

**Background**

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 (Mansell 2005). Hand in hand with these changes have appeared a loss of privacy along with threats to the security of confidential information (Riguidel et al.b 2004). ‘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.’ (Beaton & Wajcman 2004)

Trust is an issue that is often raised in discussions of privacy and security issues in technologies. Yang (Yang 2005) points out that trust is an important dimension of social capital as it is essential in relationship building. In both France and Australia, studies (Farquharson & Chritchley 2004, LeGrand et al. 2006) 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 (Farquharson & Chritchley 2004) of the attitudes of Australians to new technologies, the authors conclude that:

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

In (Rose 2005), Rose examines the concerns around information privacy in New Zealand where she determines that the greatest concern was for unauthorized access to data. She goes on to point out that individual controls (eg. choice, correction) 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.

As pointed out in (Batten & LeGrand 2006), “In 1998, Alain Weber, President of the Computer and Freedom Commission of the Human Rights League, France, stated (www.delis.sgdg.org/menu/25avril/2504aw.htm) 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 (http://www.vie-privee.org) 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.”

Previous work of the authors (Batten & LeGrand 2006) indicates that “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.” Thus, on the one hand, we have a strong empathy emerging between governments and the technology vendors, and on the other, organizations with the mandate to protect the rights to privacy of citizens.

**Methodology**

As a result of our work in (Batten & LeGrand), the authors developed a short list of questions around which to focus discussion with government and public sector representatives, including those specifically charged with privacy portfolios, in order to address some of the issues raised.

It was additionally noted that people are willing to accept a loss of privacy for the sake of convenience. One way to ensure that the convenience aspects of new technologies does not wear away at privacy expectations is to link major new systems to both legislation and policy and to put in appropriate controls. The questions for discussion were therefore:
a) What role does government play relative to security and privacy issues developing around new technologies?
b) How does policy and legislation evolve in the context of security and privacy issues developing around new technologies?

And the research team’s focus in addition to this was:
c) What are the critical differences between France and Australia vis-à-vis the above points?

Question (c) was aimed at a determination of the depth of understanding of comparative differences between Europe and Australasia; we were pleased at the extensive knowledge of some of the respondents in this regard.

Because of their roles in public office, some of those interviewed asked us to specify them by name and we have done so. A number of discussions also took place with individuals in both countries who preferred not to be named.

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

FRANCE
François Giquel, Vice-President of Commission Nationale de l’Informatique et des Libertés (CNIL), Paris, France
Economic Analysis and Statistics Division, Directorate for Science, Technology and Industry, Organization for Economic Co-operation and Development (OECD), La Défense, Paris, France

Discussions took place in either English or French as determined by the participants. The responses have been abbreviated into three general areas of questioning as delineated in the next section.

Findings

On the French side
In France, the authors spoke with CNIL, in order to understand how France as a nation dealt with security and privacy issues around technology, and also with the OECD to gain a broader perspective of the situation leading to an understanding of international interactions in resolving issues.

La Commission Nationale de l'Informatique et des Libertés, CNIL, is an administrative body established in 1978 by new 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 (from their collection, to their transportation and conservation) whenever digital techniques are being used (biometrics, video-surveillance, computer technology). There is ambiguity of responsibilities in some areas; for instance video-surveillance of public places in France is covered by a law of 1995 which in part excludes CNIL.

The Committee for Information, Computer and Communications Policy of the OECD has four working parties, one of which looks at information economy issues and another looking at security and privacy. The Information Economy unit examines the economic and social implications of the development, diffusion and use of ICTs, the Internet and e-business. It analyses ICT policy frameworks shaping economic growth, productivity, employment and business performance. In particular, the Working Party on the Information Economy focuses on digital content, ICT diffusion to business, global value chains, ICT-enabled off-shoring, ICT skills and employment and the publication of the OECD Information Technology Outlook. The OECD Working Party on Information Security and Privacy develops policy options to sustain trust, information security and privacy in the global networked society.

Q. Are you monitoring the impact of new technologies?
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 mis-use 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.

Q. Whose responsibility is it to educate on privacy and security issues?
Both the OECD and CNIL accept responsibility for education on privacy and security. In determining metrics to use in measuring government’s involvement in security and privacy, the OECD pointed out that there are problematic, and as yet unresolved, issues around defining the units for collection: what factors to include and how to get comparable readings across different countries where responsibilities may lie with either government or the private sector depending on the country, as well as confidentiality concerns. APEC is, however, keen to work with the OECD in developing a model survey for data collection.

The OECD is about sharing best practice, and so they can be helpful to ministries of communications and other groups who come for assistance. Peak or widely representative bodies are often included in discussions on security and privacy.
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?**

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.

From the perspective of the OECD, policy change is usually initiated at a specific country level, and when or if it arrives at the OECD, an attempt to gain consensus on it is made. The OECD might recommend that research and development be undertaken in a specific area, but it would never recommend a specific tool.

**On the Australian side**

In Australia, the authors talked to relevant players at the state level (in Victoria) 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; 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 of 1988. The Jurisdiction of the Privacy Commissioner of Victoria (and of other states) is limited to state and local government. Australia has introduced state level offices of privacy commissioners over the last five to seven years.

Several departments at the federal level, such as DCITA have responsibility for the IT area and associated concerns such as security and privacy. These departments work with organizations in other countries as well as trans-national ones such as the OECD, along with national groups such as the Australian Competition and Consumer Commission and the Institute for the Certification of Computing Professionals and with the state governments.

The office of Chief Information Officer in Victoria, Australia, has been in place since 2004. It oversees the use of information technology by all government departments in the State. The office of the Victorian Privacy Commissioner has particular responsibility for privacy of information. At the national level, the role of the Chief
Information Officer for AGIMO, the Australian Government Information Management Office, is to foster the efficient and effective use of ICT by Australian Government departments and agencies. AGIMO also works with governments and other bodies at the local, state, national and international levels to develop Australia's position as a world leader in e-government.

The federal government has strong mandates for security in such areas as foreign affairs, messaging and data centres. Its Department of Defence has developed an extensive manual delineating appropriate communication security practices internal to the federal government (http://www.dsd.gov.au/library/infosec/acsi33.html).

Q. Are you monitoring the impact of new technologies?
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.

Statutory functions of the Privacy Commissioner of Victoria include independent audit and monitoring of data. The websites of the Victorian Government are audited every two years to check if they are privacy compliant.

Data matching is a major threat depending on how it is done. Privacy is threatened when technologies for looking (e.g. surveillance) are combined with technologies for remembering (e.g. data matching). Examples are facial recognition and automated vehicle registration plate recognition technologies.

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 it is a constant bargain between the citizen and the State. The use of the word 'transparent' in The Act is part of the balance. The government needs to be transparent about collection, purpose and use of data. Many questions have to be raised in each context: Do we give people notice that they are being watched? What is the accountability of people who have access to this data? Is there an economic reason for keeping the data? Is there a law enforcement rationale?
Privacy is well covered at the national level through the privacy act. Banks are self-governing and follow their own code of practice; this allows them to control their costs. Identity crime is also well covered through the Act. Documents and proofs are still quite weak. This has two sides: identity fraud and collection of taxes and fines. Today, it is very difficult to track where people actually live and some use the system to avoid paying tax.

Governments have moved closer to the security end than to the privacy end of the spectrum, especially since 9/11/2001. However, 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?
People are not aware of the issues. However, awareness-raising is the responsibility of the people who provide services on the internet.
Also, there are big initiatives starting from the government level. Two levels can be distinguished: the home which is uncontrolled and the government which can be controlled. But nobody in government mandates what others are running. Therefore, there will probably be a new generation of contracts for security with large companies including audit and penalty clauses. Penalties will be used as a big stick but we will certainly prefer to use governance.

Education is also the responsibility of the home and then of the education system. Privacy commissioners have a role. Makers of products should also educate in indicating how to turn off features on their devices (e.g. how to cut off RFID tags, point out that you have a GPS device that can be used for tracking purposes etc.) 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.

The core role of DCITA is information awareness. The weak points in reality are consumer awareness and practice. Greater skills, better data management and an understanding of secure networks are needed by consumers. With the convergence of many new technologies, things are blurring and it is difficult to make decisions. The workplace is a catalyst. People are comforted by ‘protection’ of systems there and feel that they can operate in the same way in other, less well-protected, locations. Governments should raise awareness universally but it is also the role of large players such as banks, states 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.

The OECD and also APEC provide guidelines and raise awareness, but they cannot legislate.
Since 1996, the OECD has been developing surveys and key performance indicators for benchmarking and has frameworks to evaluate programs. The Australian population census is one of the first in the world to include questions on internet use.

The major issues for the near future include:

- the justice field (justice is a key role of government); information will be used to shame and punish but the debate on this is yet to be heard.
- What should be done with DNA since DNA contains personal data? DNA indicates paternity, ethnic typing, and one person's data is related to that of their blood relatives too. There are huge issues in this field.

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?**

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 several governments at state and local levels. The Australian Government Information and Communications Technology Security Manual, developed by the Defense 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, data centres, etc.

DCITA works with ACMA (the Australian Communications & Media Authority). There, they have a role in guiding policies and joint response with other agencies. They promote e-payment standards including issues of interoperability and accreditation. (Small and medium business need to be convinced that the cost of becoming standards and secure service compliant is not prohibitive.)

**Conclusions**

In responding to the key queries of this research undertaking, the following points arise from the previous section.

**a. What role does government play relative to security and privacy issues developing around new technologies?**

Governments in both France and Australia are attempting to take a lead in the deployment of new technologies and in doing so in a considered fashion with appropriate risk analysis and monitoring activities.
Governments in both countries believe they have a role in the education process, but that they are not the only parties with this responsibility. Other groups identified as being equally responsible are technology providers, users and professional educators, and some large players such as financial organizations. Government also believes that it has a mandate to gather data on technology use and to audit and monitor this use.

b. How does policy and legislation evolve in the context of security and privacy issues developing around new technologies?
Both countries recognize that private individuals are not aware of all the implications of the use of new technologies, and that policy and legislation need to be developed to protect them. Government also believes that it has a mandate to verify government department compliance with policy. A tension between conflicting roles of government was identified: the fact that government has a mandate to survey a population, alongside legitimate reasons to gather personal data (taxation, maintenance of borders, etc.).

c. What are the critical differences between France and Australia vis-à-vis the above points?
France is more advanced than Australia in the area of privacy protection. CNIL plays a very strong role in France backed by its membership of key parliamentary and judicial courts. However, privacy commissioners in Australia are developing a solid network both within Australia and internationally and are establishing themselves as important players in the arena.

Australia has defined a detailed and comprehensive set of requirements for information security (http://www.dsd.gov.au/library/infoscc/acsi33.html) as it is to be implemented at the federal level. France has less structured guidelines, but encourages self-regulation of key players through documents such as http://lesrapports.ladocumentationfrancaise.fr/BRP/984001519/0000.rtf which provides a set of case studies of the Conseil d’État.

The French government also provides educational resources for citizens through sites such as http://www.minefi.gouv.fr/dgccrf/04_dossiers/consommation/guide/guide_comm_electron_.pdf and http://internet.gouv.fr. These sites aim to educate generally about the issues surrounding new technologies. On the other hand, Australian government has concentrated on providing information about government practices and information of use to small and medium business on sites such as http://www.agimo.gov.au/practice and http://www.agimo.gov.au/information.

Out of the discussions, some major issues were identified for future attention, including the use of large interactive databases, the use of information as a means of shaming and punishment, and the introduction of DNA as a form of identification. No single entity accepts (full) responsibility for the monitoring of and response to these issues.
The authors wish to thank the Forum for European-Australian Science and Technology Cooperation (FEAST) for financial support for this research.

References