AUSTRALIAN ELECTRICAL & ELECTRONIC MANUFACTURERS' ASSOCIATION LIMITED
(ACN 008 467 481)
(ABN 80 008 467 481)
1st Floor, The Lonsdale Centre, 6 Lonsdale Street
BRADDON ACT 2612
GPO BOX 1966 CANBERRA CITY ACT 2601
TELEPHONE: (+61 2) 6247 4655 *FACSIMILE:* (+61 2) 6247 9840

28 February 2005

The Secretary
Legal and Constitutional References Committee
Australian Senate
Parliament House
CANBERRA ACT 2600

Dear Secretary

Re: Inquiry into the *Privacy Act 1988*

Thankyou for seeking the views of the members of the Australian Electrical and Electronic Manufacturers' Association, (AEEMA) concerning the effectiveness and appropriateness of the *Privacy Act 1988* to, inter alia, smart card and other privacy enhancing technologies. AEEMA is the leading industry body in Australia representing more than 400 companies supplying infrastructure, products and services in the ICT, electronics and electrical sectors.

I have attached specific responses to the Committee's terms of reference. I would like here to set out some further information about AEEMA for the Committee, and raise some matters of principle.

AEEMA's Asia Pacific Smart Card Forum, and its IT Security Forum, are the key voices for companies providing effective technologies to assist information, infrastructural and environmental security. Many of our members are actively involved in research and development into the more efficient and secure treatment of corporate and personal data, particularly in relation to the finance, health and transport industries. Please see reference material on the fora, attached.

Looking at the strategic issues of legislative application, you would appreciate that any legislative regime will often struggle to respond quickly to the host of emerging technological issues facing the community today. Regimes that endeavour to secure personal privacy or rights, would be better placed to respond to these challenges if they provided some policy context, perhaps by way of a preamble or contextualising statement which could be used in judicial and administrative interpretation to extend or limit the regime's operation.

This statement should note the broader community context in which privacy regimes operate, and *the changing nature of a society which demands ever increasing benefits*, in particular:

- community demand for increased levels of consumer convenience, especially 'linked up' services in retail, finance and health;
- increased community demand for consumer-level control of, *and access to*, personal information.

Consumers are increasingly requiring more sophisticated access services allowing efficient and effective information manipulation in retail and finance; the corresponding requirement

to confirm their identity, and seek ways to protect against that identity being compromised, can place a pressure on solution providers that sometimes appears insurmountable.

Technology such as smart card platforms offer promise in these areas, and a contextualising statement could recognise that *these consumer demands are often parallel and sometimes competing*, thus making it difficult for public policy to respond effectively to ensure a balance between competing demands. There is mounting evidence suggesting consumers are able to make sophisticated 'trade-offs' between the social goods they are seeking such as retail and banking convenience, and the balancing need for security and privacy.

This is not to suggest a weakening of privacy protections, but an acknowledgement that *they exist within a complex social environment* and that guidance may be needed to reconcile these issues. It does suggest, however, a refinement of the definition of privacy; in the past, anonymity was seen by some as the cornerstone of any privacy regime. But anonymity (literally, 'without a name' or identity) can no longer be consistent with consumer demands for increased convenience in dealing with their own data, because a *secure and verified identity is essential* if industry is to meet such consumer demands.

AEEMA is confident the Committee will review these and related matters to reach appropriate recommendations that recognise the need to balance competing demands and requirements in this complex environment. Please don't hesitate to contact Ms Loretta Johnson, Senior ICT Forum Manager and Company/Secretary at 62 47 4655 should you require any further information to assist you in that task.

Yours sincerely,

Angus M Robinson
Chief Executive

encls

Inquiry into the *Privacy Act 1988*

(a) the overall effectiveness and appropriateness of the *Privacy Act 1988* as a means by which to protect the privacy of Australians, with particular reference to:

(i) international comparisons,

It appears the legislative approach of some jurisdictions in the European Union is more highly developed, providing effective enforcement provisions and associated awareness programs for the community and business alike. Breaches of privacy are thus considered more serious than they are in Australia, and are enforced with higher penalties.

(ii) the capacity of the current legislative regime to respond to new and emerging technologies which have implications for privacy, including:

(A) 'Smart Card' technology and the potential for this to be used to establish a national identification regime,

This is an ambit assertion which is technology specific, and thus inappropriate to a policy discussion. Many other current community accepted process and systems, such as birth certificates, passports, drivers' licences and academic records could be said to contain potential for a national identification regime. Smart cards contain no more or less capacity to establish such a regime, if one were wanted, or if parliamentary governance became lax. On the contrary, they guarantee authentication and so are instrumental in ensuring privacy – the protection they provide is dependent on making data available ONLY to eligible persons. Their current use in the passport system indicates a community belief that smart cards will make passports LESS liable to fraud.

This belief is well founded, because a significant number of privacy concerns are allayed by confidence in the inherent security of the smart card, the security of the smart card application, and the security in the card accepting terminal. Each of these requires accreditation to the appropriate standards, such as ISO, APCA, ITSEC and ICAO, etc.

The essential principle is that a smart card is an authentication token.
It authenticates a right to a service (eg; a disposable, and anonymous public transit ticket), or it authenticates a User's identification.

Whatever information the business rules determine should be carried in the chip on the card, that information can be protected and kept secret. The chip hardware is tailored and optimised for this purpose, along with suitable cryptographic methods for protecting the confidential data (even if this is only a PIN, a terminal authenticating password, or a biometric identifier of the User).
The security of a smart card is ensured by four components:

1. the card body
2. the chip hardware's passive and active protection
3. the operating system
4. the application

The security of a smart card is assured only when all of these components are present and their defence mechanisms are working properly.

The smart card industry has a long history, extending back to document security even before plastic cards existed. Much of the R&D effort concentrates on simulating attack on both the hardware and the software, and developing security features that raise the barriers for attack to heights not feasible for the criminal to overcome. This is an ongoing process as electronics and manufacturing technology improves.

The proliferation of national ID programs using secure chips and operating systems on smart cards is evidence of the value in raising security levels, particularly to overcome the risks associated with fraud and identity theft. The UK, Taiwan, Hong Kong & Macao are recent examples.

Most of these do not store significant amounts of data on the chip, but rather use the advanced technology to deliver a secure "key" to access the data. That data could be financial, health, tax, traffic infringements or other confidential data, held on secure databases, and accessed by encrypted transmission sessions.

The secret to success in implementing any government-initiated smart card program will be the ability to grow consumer confidence in accepting that smart card security allays privacy concerns over access rights to personal information.

(B) biometric imaging data,

As with all technology, the extent to which biometrics threaten or enhance privacy depends on the use to which they are put. The data collected using biometric techniques is frequently stored in large databases, and it is at this stage of the process that privacy compromises could arise, because a more concerning privacy threat than technology itself, is the constant breach of database integrity through hacking and unwarranted searches. In addition, biometrics does not handle failure well. A person whose biometric data has been compromised (such as 'stolen' fingerprints) will find it almost impossible to rectify or repudiate the situation because there can be no trusted third party to issue another fingerprint. Once stolen, a biometric is stolen for life.

(C) genetic testing and the potential disclosure and discriminatory use of such information

All technology can be mis-used. Simple photographs have the potential for disclosure and discriminatory use. There is no reason to single out any specific technology, such as genetic testing, as containing any more potential for mis-use that any other.

(D) microchips which can be implanted in human beings (for example, as recently authorised by the United States Food and Drug Administration)

The use of implanted chips can be beneficial, again depending on their application and use. Accurate identification of persons in the health system for example, can obviate the risk of correct procedures being applied to the incorrect patient. The privacy regime in Australia, resources permitting, would be able to respond to such new technological developments if less emphasis were placed on singling out the technology rather than focussing on the principles of privacy enhancement, community demands for consumer convenience in banking and retail sectors, as well as demands for access to/control of personal data. Such community demands can often only be met through the appropriate application of technologies; trying to prevent the development or use of such technologies ignores the fact that it is the breach that must be stopped, not the technology. In a related sense, 'the crime is the murder, not owning the knife'.

(iii) any legislative changes that may help to provide more comprehensive protection or improve the current regime in any way;

(b) the effectiveness of the *Privacy Amendment (Private Sector) Act 2000* in extending the privacy scheme to the private sector, and any changes which may enhance its effectiveness;

A significant number of private sector organisations consider the Act to be 'guidelines' oriented only, rather than enforceable law. This results sometime sin a perceived lack of 'urgency' in implementing effective IT security measures to protect the privacy of these organisations' own customers.

An enhanced education and awareness program would go some way to overcoming this issue, which is especially apparent in smaller, less resources companies, but can also be encountered in larger enterprises.

(c) the resourcing of the Office of the Federal Privacy Commissioner and whether current levels of funding and the powers available to the Federal Privacy Commissioner enable her to properly fulfil her mandate.

Current resourcing in the Office appears insufficient in both numbers and experience to deal with the need for better awareness in the community, as well as better understanding by the Office itself of the rapid advancements in technology and their obvious benefits to business efficiency and community convenience.

In comparison with European Union jurisdictions, it would appear the enforcement powers and procedures under the Australian Act engender a more subtle approach to breaches, whereby a certain nonchalance is fostered at the community level because breaches are not considered important. The awareness program referred to above may assist to overcome this attitude.