E-Government in Australia: the Challenge to Privacy of Personal Information

MAEVE MCDONAGH

1 Introduction

E-Government is developing at a rapid pace in Australia. Indeed Australia is one of the leaders worldwide in this area. In 1997, the federal Government pledged to deliver all appropriate government services through the Internet by 2001 and this aim has been vigorously pursued ever since. At State level, Victoria in particular is involved in advanced E-Government initiatives. The privacy implications of the development of E-Government have received some attention but it is the contention of this paper that much still remains to be done to ensure that the placing of government services online does not cause irreparable damage to the privacy of Australians. The structure of this paper will be as follows:

The paper will commence with a discussion of E-Government and its various manifestations and in particular its implementation in Australia. It will then consider the threat to privacy posed by developments in E-Government. This will be followed by an evaluation of the regulatory framework for protection of privacy in Australia. Comparisons will be drawn with EU developments aimed at protecting privacy in the E-Government environment.

---

1 Senior Lecturer in Law, University College Cork, National University of Ireland. This paper is an extended and updated version of a presentation made at the National Privacy Conference, Melbourne on the 17th November 2001. Research for this paper was undertaken while the author was a visiting researcher at the Department of Law and Legal Studies, La Trobe University from September—December 2001.
2 E-Government

E-Government initiatives can be seen to operate at various levels. The first level comprises simple government to citizen communication through which government information such as reports, policy documents, legislation and case law is made available direct to the public through electronic means. In the second stage, citizen to government communication becomes possible allowing citizens to make electronic submissions concerning government proposals for example or to provide government agencies with new information about themselves, such as change of address, by electronic means. Third-level services facilitate more complex interactive transactions. These often involve legally binding procedures and/or online payments. Examples of such transactions include voter and motor vehicle registration or the submission of formal objections to applications for building permits. Such communications may involve the use of public key infrastructure (PKI). Fourth level services focus on the delivery of access to a wide range of government services across a whole government administration through a single contact point. Examples of these services are to be found in the many emerging integrated government portals. A model of portal increasingly finding favour is the citizen centric life event portal which is designed around the typical interactions citizens have with government during the course of their lives e.g. turning 18, moving house etc. At the fifth stage, yet to be fully realized in practice, government applications become intertwined with commercial applications and users are facilitated in building their own interfaces designed around their personal interactions with both government services and commercial entities.

3 E-Government Implementation in Australia

Considerable investment has been made in the development of E-Government in Australia at both federal and state levels. In 1997, the Australian federal Government promised to deliver all appropriate government services through the Internet by 2001. At federal level, the primary initiative is the Government Online Project which operates under the auspices of the National Office for the Information Economy (NOIE). As

---

2 Public key infrastructure (PKI) is the combination of software, encryption technologies, and services that facilitate protection of the security of communications and transactions on the Internet. PKI integrates digital certificates, public key cryptography, and certificate authorities into an overall network security architecture. PKI delivers the following essential elements: Privacy – the ability for confidentiality; Authentication – the capacity to establish identity; Integrity of data – to ensure that data has not been altered; Non-repudiation – to provide irrefutable evidence that an action has occurred.

part of its strategy, the federal Government has also created the Gatekeeper PKI framework to allow for the accreditation of certification authority service providers and their public key technology products in order to facilitate web based transactions. The NOIE is responsible for managing Gatekeeper. At State level, Victoria has led the way in implementing E-Government. Victoria currently has in place two portals which allow access to a wide range of government information and services, Multi Service Express and MAXI.

International surveys of E-Government activity have placed Australia amongst the most advanced nations in the world. The Accenture survey of 'E-Government leadership' undertaken in April 2001 which examined the quality and presentation of government services on-line ranked Australia 5th out of the 22 countries surveyed.\(^5\) A survey undertaken by Brown University in the US for WMRC (World Markets Research Centre) in August 2001 ranked Australia 2nd in the world behind the United States in terms of availability of government information and services online.\(^6\)

At domestic level, surveys have been undertaken as part of the federal Government Online Project to determine the level of progress of Commonwealth agencies towards the aim of implementing all services online before the end of 2001. The most up to date results available are those of the October 2001 survey.\(^7\) The survey identified 3 different levels of sophistication in services namely:

- Services that provide static information only;
- Services that provide access to downloadable information; and
- Services that involve integrated transactional/informational services.

The first three stages of the five stages of development of E-Government described earlier encompass these three levels. The survey showed that of the online services offered by government agencies: 27% were services that provided static information only; 43% were services that provided access to downloadable information; and 30% of services were provided at the integrated transactional/informational services level.

In terms of the use of PKI technology by government agencies in their interactions with clients, this appears to have been largely confined at federal level to a small number of agencies such as the Australian Tax Office and the Health Insurance Commission. In Victoria, the MAXI system relies in part on the use of a digital certificate which is issued by a commercial certification authority.

4 E-Government and the threat to privacy

The volume and sensitivity of personal information collected by government websites depends to a great extent on the level of sophistication of the E-Government application. Government websites which operate at the lowest level, namely that of government to citizen communication, will collect little if any personal information. At the more complex levels, such as those of citizen to government communications and the use of websites to undertake complex interactive transactions, large volumes of often sensitive personal information is collected. Where integrated portals have been put in place in order to facilitate access to a range of government services, a wide variety of personal information is collected and this is sometimes stored at a central location. The introduction of public key infrastructure (PKI) technology gives rise to a range of additional problems.\footnote{Greenleaf, and Clark, 'Privacy Implications of Digital Signatures' available at \url{http://www.anu.edu.au/people/Roger.Clarke/DV/DigSig.html}.} It is clear that as E-Government initiatives become more complex, pervasive and integrated, the issue of ensuring privacy of personal information in the E-Government environment will become ever more pressing.

Many of the privacy problems which arise from E-Government applications are the same as those which arise in the online commercial context. They focus on matters such as:

- the method of collection of personal information;
- use of personal information;
- disclosure to third parties of personal information collected about individuals;
- security of personal information held by government agencies.

4.1 Collection

In terms of the method of collection of personal information, the issues which generate most concern are those of:

- automatic collection of personal information without reference to the individual concerned, for example by means of cookies on websites;
- other intrusive practices with regard to collection of personal information either from the individual concerned or from third parties e.g. collection of e-mail addresses on websites and their inclusion in mailing lists;
- application and registration processes for public key technology products such as digital certificates.
4.2 Use & Disclosure

The main focus of controversy surrounding use and disclosure of personal information in the online environment is that of consent. Information which has been collected by a government agency via a website may be easily transmitted to another agency or even to the private sector. This will be greatly facilitated by the development of integrated portals. In the PKI context, there is concern about function creep and in particular about the emergence of a de facto national identifier. This could happen where individuals use the one digital certificate in their dealings with all agencies (and possibly also with private sector organizations). The agency might record some feature of the certificate with other records of personal information about the person. This would facilitate matching of personal data about the individual across a range of situations.

There are also privacy concerns relating to the use of public key directories. These include the possibility that data could be downloaded from such directories. The downloading of digital certificates from a public key directory could, for example, reveal an association of an individual to a particular agency. Public key directories may contain e-mail addresses and the potential for the harvesting of e-mail addresses for spamming purposes also gives rise to concern. Concerns also arise in respect of certificates revocation lists (CRLs). For example publication of the reasons for revocation of digital certificates may disclose personal information.

4.3 Security

Security issues exist where secure infrastructure for the transmission of personal information is absent. The security of private keys in the PKI environment gives rise to particular concern. If the security of private keys is not protected it will leave subscribers open to serious invasions of their privacy. It can, for example facilitate identity theft i.e. allowing others to impersonate them in their dealings with agencies.

While similar problems arise in the online commercial context, the difficulties which arise may be exacerbated by the fact that the interactions are taking place with government agencies. This is because citizens do not generally have any real choice as to whether to engage in such interactions or not. Also most citizens interact with a range of government agencies thus increasing the likelihood of the exchange of information between agencies.

---

9 A certificate revocation list (CRL) is a list of certificates that have been revoked before their scheduled expiration date. There are several reasons why a certificate might need to be revoked and placed on a CRL. For instance, the key specified in the certificate might have been compromised or the user specified in the certificate may no longer have authority to use the key.
5 Australian privacy laws in the E-Government environment

The principal privacy protection law applicable to the public sector at federal level in Australia is the Privacy Act 1988. This Act established 14 information privacy principles (IPPs) based on the Guidelines adopted in 1980 by the Organisation for Economic Cooperation and Development (OECD) for the Protection of Privacy and Transborder Flows of Personal Data.\(^{10}\) At State level, the only States to have instituted a public sector privacy regime to date are Victoria.\(^{11}\) and New South Wales.\(^{12}\) The approach of both Acts is largely modeled on the federal privacy regime. The IPPs and the OECD Guidelines on which they are based set out a framework for the protection of information privacy and are not very detailed. One advantage of the privacy principles approach is that it is adaptable and does not readily become out of date. However a disadvantage of this approach is that it leads to uncertainty as to what practices are permissible within its terms. The applicability of these principles and the OECD Guidelines on which they are based to the online environment has also been questioned by various commentators.\(^{13}\)

The information privacy protection principles of most relevance to the operation of government websites are IPPs 1, 2, 3, 10 and 11 which deal with the collection, use and disclosure of personal information.

In its November 2000 report *CookieMonsters? Privacy in the information society*, the Senate Select Committee on Information Technologies identified a number of problems regarding the operation of the Privacy Act in the online environment. Chief amongst these were the scope of the definitions of personal information and the issue of consent.

5.1 *The definition of personal information*

Personal information is defined in the Privacy Act 1988 as

... information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can be reasonably ascertained, from the information or opinion.

The Report suggests that cookies are not covered by this definition.\(^{14}\)

---

\(^{10}\) OECD recommendation concerning and guidelines governing the protection of privacy and transborder flows of personal data, O.E.C.D. Document C(80)58(Final), October 1, 1980.

\(^{11}\) Information Privacy Act 5900 (Vic.) No. 98 of 1990.


---

332
The basis of this assertion appears to be that the identity of the individual will not be apparent from the cookie. This is because the cookie only identifies users via a user number. However the definition also applies where the identity of the individual could reasonably be ascertained from the information. Combining the cookie with information from other sources could reveal the identity of the individual concerned and so a case can be made for the proposition that cookies come within the definition of personal information for the purposes of the Privacy Act. However this is still an area of uncertainty and it would be better if it were clarified through legislation. The Senate Report refers to the definition of personal information in the EU Data Protection Directive as being more explicit its application to technological developments such as the cookie, the main difference between the definitions being that the EU definition explicitly covers situations where a person may be indirectly identified.

Another significant development at EU level is the Directive on the processing of personal data and the protection of privacy in the electronic communications sector. This Directive, which applies to publicly available electronic communications services, includes a provision which limits the use of cookies by requiring Member States to offer to subscribers or users the right to refuse such processing except where it is required for technical reasons or where it is strictly necessary in order to provide an information society service explicitly requested by the subscriber or user. The proposed Directive also requires that, subject to certain exceptions, traffic data relating to subscribers and users which is processed and stored by the provider of a public communications network or publicly available electronic communications service, should be erased or rendered irreversibly anonymous upon completion of the transmission.

5.2 Consent

On the issue of consent to the collection, use or disclosure of personal information, the Senate Select Committee’s Report emphasised the need for individuals to understand fully the nature of their consent and its ramifications. The report identified the following conditions as essential to the provision of meaningful consent:

16 Article 3 of the Directive provides that ‘personal data’ shall mean any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
18 This is defined as ‘Any personal data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof’.
• knowledge of privacy and opt-out rights;
• restrictions on blanket consent;
• assurance of ongoing privacy protection; and
• practical access to privacy policies and practices.

The principal difficulties with the definition of consent in the Privacy Act is that it includes implied consent. This means that the operator of an agency website would be able to argue for example that the use by the citizen of the web based service amounted to the giving of his or her implied consent to the transmission of personal information collected in the process to other government agencies or even to private sector organizations. The definition of consent in the EU Data Protection Directive by comparison requires that consent to the collection of personal information be explicit. Consent is defined in the Directive as ‘any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.’

5.3 Other problems with the IPPs

Other problems with the application of the IPPs to the E-Government environment include the fact that they allow the provision of information regarding collection of personal information to take place after the information has been collected from the individual concerned. IPP2 merely requires the collector to take reasonable steps to ensure that the required information is supplied either before the personal information is collected or, if that is not practicable, as soon as practicable after the information is collected. Thus a collection of personal information via a website could take place in compliance with IPP2 without the individual concerned being informed of matters such as the purpose to which the information would be put or the third parties to whom it would be disclosed. Another difficulty lies in the fact that personal information contained in what are referred to in the Privacy Act as ‘generally available publications’ is largely unprotected. In particular, the limitations on disclosure, use and the requirements relating to security do not apply to such information. The only IPPs to apply to personal information in generally available publications are those relating to collection. Generally available publication is defined to mean a magazine, book, newspaper or other publication (however published) that is or will be generally available to members of the public. A government website could clearly fall within the scope of this definition unless it were secured in some way as to prevent access.

19 Article 8.
In the PKI context, registers of public keys or certificates are likely to be viewed as generally available publications, thus leaving them largely outside the protection of the IPPs. Other PKI related problems not addressed by the IPPs are the need to ensure that the use of PKI remains voluntary and that individuals be allowed to conduct anonymous transactions and to hold multiple keys.

6 Privacy Commissioner Guidelines

In May 1999, in the exercise of powers conferred on him by the Privacy Act 1988,\(^{20}\) the federal Privacy Commissioner issued guidelines\(^{21}\) for federal and ACT government websites. The Government included the guidelines in its Government Online strategy and required agencies to comply with them by 1 June 2000. There are four main guidelines. The first recommends that government websites should incorporate a prominently displayed privacy statement. The privacy statement should state what information is collected, for what purpose and how this information is used, if it is disclosed and to whom, and should address any "other relevant privacy issues". While the guidelines question whether cookies amount to personal data for the purposes of the legislation, it is recommended that website privacy statements state what cookies are used and for what purpose.

The second matter addressed in the guidelines is that of collection of personal information via websites. The Privacy Commissioner recommends that agencies that solicit or collect personal information via their websites should comply with IPPs 1–3 and that agency website privacy statements should include a statement regarding collection which complies with IPP 2. Where an online form is used to collect personal information it is recommended that the privacy statement be on the same page as the form or prominently linked to it.

The issue of security is dealt with in Guideline No.3. It recommends that where personal information is collected via a website, this should be done by "sufficiently secure means". The Guidelines also recommends that individuals be provided with alternative means of providing personal information and that security measures should be addressed in the website privacy statement where appropriate.

Finally the guidelines recommend that where agencies are considering the publication of personal information regarding individuals on the web,

\(^{20}\) s271(1)(e).

they should be sure that this complies with IPPs 1–3 and 10 and 11. The Commissioner suggests that agencies should carefully consider the appropriateness of publishing personal information on the web as this information may be exposed to a much wider audience than was originally intended.

A major problem with guidelines issued by the Privacy Commissioner is that of the uncertainty of their legal status. The legislative basis of the publication of such guidelines is section 27(1)(e) of the Act which gives the Commissioner the power:

e) to prepare, and to publish in such manner as the Commissioner considers appropriate, guidelines for the avoidance of acts or practices of an agency or an organization that may or might be interferences with the privacy of individuals or which may otherwise have any adverse effects on the privacy of individuals;

The Act does not directly address the issue of enforcement of guidelines issued under this provision. The Guidelines appear therefore to be merely advisory.

The problem of enforcement is borne out by the Privacy Commissioner’s own survey of compliance with his Government Web Site Guidelines. A study undertaken in July 2001 study revealed that the proportion of Commonwealth websites that display privacy statements has increased from 18% in 1999 to 68% in 2001. While the Commissioner welcomed this increase, he said that it was a matter for concern that nearly a third of Commonwealth websites still did not display any privacy statement. Other findings of the survey were that less than one quarter (21.6%) of all websites that collect personal information had an adequate IPP2 statement or a direct link to a privacy statement and that less than half (42%) of all websites audited warned users of the risks of transmitting data across the Internet. The survey further revealed that only 2.8% of sites audited used encryption methods to ensure secure transmission of personal information and that three quarters (75.2%) of all websites audited display personal information about agency staff. This included information relating to names, photographs, work addresses, work and mobile phone numbers, facsimile numbers and biographical details.

The Privacy Commissioner’s Guidelines for Federal and ACT Government web sites can be compared with those recommended by the Data Protection Working Party of the European Union under Article 29 of the EU Data Protection Directive. The Article 29 Recommendation which was adopted in May 2001, sets out guidelines primarily in the areas of

---

22 See, for comparison, section 135AB of the National Health Act 1953 which provides that breach of the Medicare and Pharmaceutical Benefits Privacy Guidelines amounts to an interference with Privacy for the purposes of the Privacy Act.

23 Recommendation on certain minimum standards for collecting personal data on-line in the European Union adopted 17 May 2000 5620/01/EN/Final.
collection of personal information online. It focuses both on the substance of the information to be provided and on the manner and timing of the provision of such information. While the guidelines are in the form of a recommendation and are therefore not legally binding, the EU Directive contains measures which render such recommendations more susceptible to enforcement than their Australian counterparts.24 Specifically the Directive provides that the Working Party’s recommendations shall be forwarded to the European Commission and the Commission is obliged to inform the Working Party of the action it has taken in response to its recommendations. The response must be contained in a report which must be forwarded to the European Parliament and the Council. The report must also be made public.

The main differences between the EU Recommendation and its Australian counterpart are:

- The unequivocal EU requirement that information regarding collection of personal information online be provided prior to the collection of such information.
- The scope of the information disclosure requirements at the time of collection provided for in the EU Recommendation. These extend beyond those provided for in the Privacy Commissioners Guidelines to require disclosure of the following:
  - the identity and physical and electronic addresses of the person collecting the information;
  - whether supply of the information is optional or compulsory;
  - the rights to consent or object to the processing of personal information and to access, rectify and delete such information;
  - the purpose of the supply of personal information to third parties. The Privacy Commissioner’s Guidelines only require the identity of such recipients to be disclosed.
  - the requirement that users be given the opportunity to object to the transmission of information to third parties by means of an opt-in mechanism i.e. where the information will only be passed on where the user clicks a box in support of disclosure.
  - the more extensive information to be provided with regard to any automatic data collection processes in place (such as cookies or clickstream data) including details such as the domain name of

24 Article 30.
the site server transmitting the automatic collection procedures, the purpose of those procedures as well as information on the option available to the user to object to their use. The Recommendation makes it clear that such information must be provided before any automatic procedures are triggered.

- the security measures in place on the site
- a requirement that effective measures be put in place for exercise of the rights to access and to rectify information and that the exercise of such rights should be possible both at the physical address of the holder of the information and online.
- a requirement that anonymous or pseudonymous consultation of websites be allowed wherever possible

7 PKI privacy protections

Efforts have been made in Australia to address privacy concerns generated by development of PKI on two fronts. In the first place, various privacy requirements are included in the Gatekeeper framework itself. The Gatekeeper protections apply in respect of the relationship between the agency and the individual client and also to the activities of certification and registration authorities. In addition the federal Privacy Commissioner published a set of guidelines for agencies using PKI in December 2001. These guidelines focus on privacy aspects of the use of PKI by agencies for the provision of services to individual clients.

7.1 Gatekeeper Privacy Requirements

The government’s PKI strategy, Gatekeeper, imposes privacy requirements on those wishing to be accredited under the system. These requirements apply to bodies in the trust framework that confirm identity (registration authorities) or issue certificates (certification authorities). The Gatekeeper rules do not apply directly to the government agency/client relationship.

The standard Gatekeeper agreement requires Certification Authorities (CAs) and Registration Authorities (RAs) to abide by the IPPs. In addition the accreditation requirements for both CAs and RAs mandate compliance with certain privacy standards as a condition of accreditation. Additional privacy requirements were introduced in May 2000 and these have also

---

25 Certification Authorities (CAs) issue and revoke digital certificates while Registration Authorities (RAs) conduct the initial verification of a potential subscriber’s identity and/or attributes.

338
been incorporated into the Gatekeeper accreditation requirements. Many of these Gatekeeper privacy requirements are more specific and far-reaching than the demands of the IPPs. For example, the Gatekeeper privacy standards require that PKI designs have, amongst others, the following features:

- That they allow subscribers to have multiple certificates from the same CA, wherever the use of multiple certificates is not inconsistent with the purpose of those certificates.
- That they give subscribers a choice in relation to the accredited issuer of certificates and the private key and certificate storage.
- That they ensure that there is no centralised storage of PKI distinguishable name or identification details.
- That they ensure that individuals are only subjected to appropriate identification procedures and that intrusive procedures are minimised to the extent possible.
- That they incorporate effective privacy controls over the information contained in Certificate Revocation Lists and how CRLs are accessed and searched.
- That the CA have the ability to provide anonymous or pseudonymous certificates where appropriate.
- That they include privacy protection relating to CRLs and other directory services including requirements that no personal information be made publicly available in CRLs and other directory services and that CAs collect and hold minimal personal information when logging accesses to CRLs or other directory services.

The scope for enforcement of these requirements is limited however. Failure to abide by the accreditation requirements can lead to revocation of the accreditation or to an action for breach of contract both of which courses of action would have to be initiated by NOIE. There is however no scope for an aggrieved party to make a complaint to the Privacy Commissioner or any other forum where he or she suffers as a result of breach of these standards.

7.2 *The Privacy Commissioner’s PKI Guidelines*

These guidelines were formulated following the issuing by the Commissioner of a Consultation paper on this topic in June 2001.27 The

---

Consultation paper identified a number of privacy concerns around the operation of PKI. They included matters such as:

- the intrusiveness of the registration process;
- the extent of personal information contained in digital certificates;
- the danger to privacy posed by public key directories;
- the logging of transactions;
- security of private keys;
- the potential for PKI to facilitate the development of a de facto national identifier;
- function creep i.e. the accumulation of additional uses for certificates;
- the right to choose not to use PKI;
- the need to facilitate anonymous or pseudonymous transactions;

There are nine guidelines in all. The first requires that the use of PKI be voluntary and that clients be offered alternative means of service delivery should they not wish to use PKI and that the risks and benefits of PKI and alternative methods be disclosed. This is an important protection. The commentary on the guideline states that clients should have the choice not to participate in PKI for a particular transaction subject to any legislative requirements. This leaves it open for the introduction of legislation mandating the use of PKI. Guideline 2 deals with awareness and education. It requires agencies and PKI service providers to cooperate closely to ensure that clients are fully informed of the proper use of PKI. Four alternative methods of delivery of such education and awareness are suggested. The focus is very much on client rather than agency responsibility for the security of private keys although one of the alternative approaches suggested notes that agencies ‘could consider’ that they are not simply transferring risk to clients by providing them with security information. Guidelines No.3 requires agencies to undertake a Privacy Impact Assessment (PIA) before implementing a new PKI system or significantly extending an existing PKI system. A sample PKI PIA is provided to assist agencies in meeting the requirements of this guideline. The use of privacy impact assessments was pioneered by New Zealand and by certain Canadian provinces. It is a useful tool in identifying privacy issues which may arise in the implementation of new systems. The Privacy Commissioner’s guideline proposes that the PIA be undertaken by the agency proposing the new PKI system. However as O’Flaherty points out, ‘internal advocates of innovative systems are naturally reluctant to be too
critical of their scheme’. Agency personnel may not, in any case, be sufficiently familiar with data protection standards to be able to undertake such a task. Some of the questions set out in the draft PIA published with the Privacy Commissioner’s guidelines include the following: ‘Is the personal information being collected by lawful and fair means?’ and ‘Will the information collected not intrude to an unreasonable extent on the personal affairs of the individual.’ No guidance is given with regard to the answering of these questions. It is clear that a full understanding of data protection principles would be needed to enable a complete answer to be given. Another issue which is not addressed in the Guidelines is what happens to the PIA once it has been conducted. The Guidelines recommend that it be integrated into the decision-making process surrounding the PKI application under proposal but it is not clear, for example, whether the Privacy Commissioner is to have a role in approving the finished product.

Guideline 4 addresses the issue of the amount of evidence of identity (EOI) which should be required of clients who will be using PKI applications. The guideline states that agencies should ensure that only minimum EOI that is necessary for, or directly related to the process should be collected. To avoid requiring clients to undergo multiple EOI processes in order to interact with a range of agencies, one of the options put forward is that a single EOI process could be used, subject to the client’s consent, for the generation of multiple certificates. While this might be convenient it raises issues with regard to the different levels of identification needed for various transactions. It could result in the passing of irrelevant personal information between accredited gatekeeper providers. Guideline 5 is concerned with the potential for the compilation of detailed histories of client transactions by agencies and PKI service providers in the course of the operation of PKI applications. It provides that such histories should not be created or used ‘except to the extent required for system maintenance or evidentiary purposes’. There is no further explanation of the phrase ‘evidentiary purposes’ but the discussion which follows envisages the disclosure of aggregated logs relating to individuals where this is deemed to be reasonably necessary for law enforcement or the use by agencies of aggregated information about its staff or a client for similar purposes. Such disclosures and uses, it is recommended should only take place in conformance with the requirements of IPPs 10 and 11. Guidelines 6 states that agencies should allow clients to use more than one certificate, where these are fit for the purpose of the relevant application and that agencies should recognize certificates

which have not been issued by them. The implementation of this Guideline would be an important barrier to the development of a national identifier. Given the natural tendency toward function creep it would be preferable if this guideline were to be stated in stronger terms, for example by requiring agencies to inform clients about the benefits to them of engaging with agencies through multiple rather than single certificates. Guideline 7 deals with subscriber generation of keys. It provides that clients should be given the option of generating their own keys subject to the agency being satisfied that the key generation can be implemented securely. The advantage of this in terms of privacy is that it helps to ensure that the private key is available only to its owner. The Guideline does not go so far as to require that software which allows subscriber generation of keys be made available. The suspicion that this guideline amounts to no more than lip service to the concept of subscriber generation of keys is supported by the admission in the commentary following the guideline that there is no product currently on the list of software products required to be used for the purpose of key generation by the Gatekeeper policy which allows for subscriber generation of keys. Guidelines 8 is concerned with public key directories. It requires that agency clients be allowed to opt out of including their public keys in a public key directory (PKD) where the PKD is published. In the commentary which follows this guideline, the question of the need for PKDs to be published is explored. It is clear from the discussion that this is not always necessary. It would have been preferable therefore if the Guideline had required agencies to consider, as a first step, whether the PKD should be published at all. There is no guideline concerning Certificate Revocation Lists (CRLs), the potentially privacy invasive aspects of which have been referred to earlier in this paper. Guideline 9 provides that agencies should provide their clients with anonymous or pseudonymous options for transacting with them to the extent that this is not inconsistent with the objectives and operation of the relevant online application. While this is laudable as far as it goes, agencies should be required to inform clients of the availability of such options where they exist. Interestingly, as the commentary acknowledges, Gatekeeper does not currently support anonymous transactions. The circumstances in which the use of anonymous or pseudonymous certificates would be permitted should be more explicitly stated. The guideline itself uses the vague formulation of allowing such an option where ‘this is not inconsistent with the objectives and operation of the relevant online application’ while the commentary appears to favour a narrower set of circumstances in which use of anonymous or pseudonymous certificates should be refused. It refers to the need to use identity certificates to ensure non-repudiation of statutory or contractual transactions and to the need to comply with legal requirements on agencies and their clients.

The same issues with regard to enforceability of the Privacy Commissioner’s guidelines arise in respect of the PKI Guidelines as were raised
earlier in the discussion of the Commissioner’s guidelines for government websites.

8 Conclusion

To conclude, it is clear that Australian privacy law is inadequate to protect privacy in the e-government environment. While efforts have been made to address some of the issues raised by the development of e-Government generally, and the adoption of PKI applications in particular, the standards which have emerged suffer from a range of shortcomings and, in any case, are not fully enforceable. Much investment is going into the development of E-Government in Australia and it is clear that developments in this area will continue to proceed at a relentless pace. These issues need to be addressed in the immediate future as once these expensive and undoubtedly efficient and convenient systems are fully implemented there will be significant resistance to altering them in order to undo or limit the damage to personal privacy. Unless the deficiencies in the regulatory regime are addressed, irreparable damage to personal privacy will ensue which in turn will operate to undermine public confidence in E-Government initiatives.\textsuperscript{29}

\textsuperscript{29} Failure to address these issues could also damage Australia in terms of its interactions with governments in other parts of the world such as Europe. The EU Article 29 Data Protection Working Party has already issued an opinion in which the Australian private sector privacy regime was found to be inadequate in terms of meeting EU standards (Opinion 5/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000, 56/1/2001). Given that the national privacy principles (NPPs) on which the private sector system is based are more demanding than the IPPs it is clear that the IPPs would be found similarly wanting.