COMPUTERS & LAW

Journal for the Australian and New Zealand Societies for Computers and the Law

Editors: Belinda Justice and Claire Elix

ISSN 08117225

Number: 56

June 2004

Parliamentary Report highlights Commonwealth IT Legal Issues

Gordon Hughes, Blake Dawson Waldron

Gordon Hughes is a partner at Blake Dawson Waldron. He is a former president of the Victorian Society for Computers and the Law and is co-author with Anna Sharpe of "Computer Contracts: Principles and Precedents"

Synopsis

A Commonwealth parliamentary committee recently published a report regarding the management and integrity of electronic information in the Commonwealth public sector. The committee's recommendations were wide ranging. This article focuses on issues which are likely to be of immediate interest to IT lawyers – principally, comments made by the committee in relation to IT outsourcing contracts, public key infrastructure and open source software.

Introduction

On 1 April 2004, the Joint Committee of Public Accounts and Audit published a report entitled *Enquiry into the Management and Integrity of Electronic Information in the Commonwealth* ("Report 399").

The committee had been established to enquire into the potential risks arising out of the manner in which the Commonwealth collected, processed and stored private and confidential data, and the terms of reference specifically focussed the committee's attention on privacy and confidentiality issues and the adequacy of the current legislative and guidance framework.

The report made nine recommendations in all. The findings have been described in the media as representing a "comprehensive failure" by the Federal Government in relation to e-security. This may be something of an exaggeration but in any event this article is not intended to focus upon, or to evaluate the implications of, each of the recommendations regarding the

Continues page 3

In this issue:

Continued from page 1

manner in which the committee considered that data security could be enhanced.

Instead, this article will focus upon three issues which are likely to be of direct interest to lawyers:

- Recommendation 2, which recommended the inclusion of certain provisions in outsourcing contracts to ensure the adequate protection of Commonwealth data;
- Recommendation 9, which recommended a review of the Commonwealth Gatekeeper initiative; and
- comments made by the committee on the relative merits of closed and open source software.

Recommendation 2 – IT Outsourcing Contracts

Recommendation 2 stated that:

> *The Australian Government Information Management Office advise all Commonwealth agencies that new or renegotiated contracts for outsourcing of information technology services need to pursue best practice and include the following:*
>
> - *clear information sharing protocols that require each party to inform the other when an information technology security incident occurs that, directly or indirectly, affects the security of agency information technology networks;*
> - *prohibition of unauthorised subcontracting of information technology services;*
> - *provision for a graduated hierarchy of sanctions in response to security breaches.*

Submissions received by the committee indicated that there were a number of management concerns arising out of the outsourcing of IT services, including:

- adverse impacts that the security requirements of one agency can have upon the security requirements and cost effectiveness of other agencies when they are inappropriately grouped together under clustered contracts;
- failure to specify expected service levels and clear performance indicators in contracts;
- uncertainty of access to Commonwealth data held by outsourced service providers;
- costs and inefficiencies caused by service providers setting passwords; and
- lack of monitoring of outsourced service providers for compliance with their privacy obligations.

In relation to the recommendation regarding information sharing protocols, the Committee's concerns emanated essentially from its perception that, with the rapid growth of on line services, it was important for Commonwealth agencies to set a high standard of integrity and privacy in administering the data which they held, and that it was equally important for the public to be aware that this high standard was being applied. It was emphasised that the onus was on agencies to not only protect the information which they held for the sake of its value to the Commonwealth, but also to protect the privacy of the individual whose information was being held. Whilst elsewhere the report emphasised concerns about physical security issues raised by outsourcing, it would not appear that flow-on risks as between agencies was a perceived shortcoming in existing contracts. Indeed there are obvious limitations on the extent to which the issue could be effectively addressed through contract as opposed to, for example, through encouraging information exchange between Commonwealth agencies regarding their IT outsourcing experiences.

In relation to the recommendation regarding unauthorised subcontracting, again the committee's approach appears to have been precautionary rather than a response to any identified inherent deficiency in existing contracting practice. For example, the Australian National Audit Office (ANAO) submitted that provisions preventing the main contractor from subcontracting without the knowledge and approval of the Commonwealth agency should be a standard part of outsourcing contract, adding as a rider that "in practice, that was generally the case and .... subcontractors are normally required to sign non-disclosure agreements and [are] prohibited from using the equipment for other clients unless specified requirements are met".

In relation to a graduated hierarchy of sanctions for security breaches, the committee's findings emphasised an inherent difficulty with outsourcing arrangements that is not confined to the Commonwealth and that, indeed, is not confined to the consequences of security breaches. This relates to the fact that, when confronted by breach, termination is often an unrealistic option for the customer to pursue, given the investment in the outsourcing relationship, the criticality of the service provider's work and the fact that physical resources used by the service provider may be owned by the service provider and may not revert to the customer upon termination. The need for the introduction of innovative and effective sanctions – typically in the form of service rebates but sometimes in more imaginative ways, such as the automatic extension or truncation of contract terms – continues to be a prime focus of contract negotiations in all IT outsourcing contracts.

The committee concluded that any agency electing to outsource its IT functions had a prime responsibility to ensure that its contracts "are tightly written and well managed". The committee expressed concern that many agencies still face "a considerable amount of work to achieve best practice in this area".

It would be reasonable to surmise that the committee accurately identified a number of challenges which typically arise in any IT outsourcing contract negotiations. Whilst the report correctly observes that IT outsourcing contracts need to address such issues with as much thought and precision as possible, it also concedes that at the

end of the day, contracts can effectively only impose sanctions and cannot guarantee actual compliance – compliance is ultimately a matter for contract management rather than contract content.

Recommendation 9 – Gatekeeper

Recommendation 9 stated that:

> *The Department of the Prime Minister and Cabinet should review and report to the Committee on the cost effectiveness of Gatekeeper verses other commercially available public key infrastructure products and systems*

The Commonwealth government's "Gatekeeper" strategy was launched in 1998. It is a national framework for the use of public key technology and for securing electronic transactions between Commonwealth agencies and users.

Pursuant to this strategy, the Gatekeeper Policy Advisory Committee (GPAC) was created. GPAC operates an accreditation system which is designed to provide accreditation to a range of electronic service providers, including (but not limited to) certification authorities. The intention, therefore, is that users can achieve some measure of reassurance that a certification authority is reliable on the basis that it must have satisfied the GPAC accreditation process.

The Committee heard evidence on the limitations of Gatekeeper, in terms of cost and security.

PKIs such as Gatekeeper were described as "... not a foolproof solution to identity management". If a person's private keys were compromised, unauthorised people could impersonate them or read or their messages. Private key security is of course of paramount importance to users of PKC, and this was highlighted to the committee as a crucial weakness of the PKC system as currently used, due to the fact few key holders can guarantee the absolute security of their keys. Private keys may be the target of crackers, viruses or worms. Hardware and software systems currently provide very little in the way of security features.

The committee noted that there were several companies claiming to be able to provide a system which could at least match the security and performance of Gatekeeper. Some systems, it was claimed, could also be supplied at lower cost.

The committee concluded that, ultimately, the decision on an appropriate system lay with the chief executive of each agency, provided that the chosen system met the security standards suitable to its purpose. The committee urged all agencies to weigh other options against Gatekeeper when reviewing their security needs, and to carefully assess the costs and benefits of each system before reaching a decision.

Specifically, the committee commented that "Gatekeeper appears to be an expensive, technically successful PKI for ensuring the privacy, integrity and security of electronic information transmitted by Commonwealth agencies, despite its low take-up by agencies generally". The take-up was likely to improve if the cost of Gatekeeper to users were reduced and if the use of the Internet as a communication medium between agencies, and between agencies and their clients, were to expand.

Closed Versus Open Source

The committee did not make specific recommendations in relation to the relative merits of closed and open source software, but its discussion is instructive given current debate on the topic.

Specifically, the committee observed that "agencies should consider the benefits or otherwise of using open or closed source software, as a normal part of their IT risk management processes and their cost/benefit analysis of new resources".

The merits of open source software, particularly in the context of government procurement, have been the subject of considerable debate in recent times. On 10 December 2003, the ACT Legislative Assembly passed the *Government Procurement (Principles) Guideline Amendment Act* 2003 regarding the use of open source software by ACT government entities. Previously, on 18 September 2003, the Australian Democrats introduced into the Senate a Bill dealing with open source software – the *Financial Management and Accountability (Anti-restrictive Software Practices) Amendment Bill* 2003 – which purported to require all Commonwealth government agencies, wherever practicable, to procure and use open source software in preference to proprietary software.

Such legislation is intended to address the perceived disproportionate and restrictive hold on the supply, use and development of software, particularly by Microsoft, within the public sector. It tends to open up debate, however, as to the reliability and security associated with open source.

The committee observed that protection of computer systems from attacks from outside was a vital part of the terms of reference for the inquiry, and noted that there was "a strong body of opinion that the Commonwealth's ability to protect its computer networks would be enhanced if open source software were in general used by Commonwealth agencies".

The committee was presented with extensive material on the relative security capabilities of closed source software on the one hand and open source software on the other. The report noted that evidence given on this issue had divided itself into the two camps, "with little common ground".

Supporters of closed source software claimed that the security features of closed source products were subjected to a more rigorous production and testing regime and were superior to comparable open source programs.

Supporters of open source software claimed that the transparency of the source code of these products allowed them to be extensively tested by a wide range of independent users – the so-called "many eyes" theory. This process, they claimed, resulted in many vulnerabilities being found and repaired before a major problem could occur.

Key participants in the debate before the committee were the Australian

UNIX and Open Systems Users Group (AUUG) on the one hand, and Microsoft on the other.

AUUG emphasised that the use of standard, open protocols across a network allowed a wide range of software, hardware and communications products to interact successfully. If reliance were placed on one proprietary, closed source application, such as Microsoft Word, then all other users were committed to using that same product if they wished to have access to the data.

AUUG argued that independence from a particular vendor was an advantage. As cited the report, AUUG urged that: "Software vendors may go out of business, may increase prices to an unacceptable level, or may decide that it is no longer in their business plan to support the software". In the long term, this could lead to data becoming inaccessible.

Microsoft countered by asserting that data stored in its closed format would still be accessible in 100 years time and that it was in the company's best interest that compatibility was maintained so that customers could see value in upgrading to a new version and could be confident that they would have the ability to bring forward their documentation.

On the specific question of the security merits of open source software compared with closed source software, AUUG stated that ". . . access to source means that an enormous amount of peer review goes on" and that "... the fact that it is available means that it is looked at by a very broad number of people from different educational and cultural backgrounds, and that diversity leads to a lot of, out-of-the-box thinking; therefore a lot of problems are found proactively and are fixed".

Microsoft countered this argument by saying that security requires highly qualified experts to actually examine, fix and test code. It claimed that simply making source code available to volunteer programmers was not enough, and widespread source code availability itself could introduce security risks.

The committee concluded that "the debate between the proponents of closed and open source software seems likely to continue with no decisive advantage to either side" and that there were strong arguments for both sides of the debate. Nevertheless the Committee considered it appropriate to acknowledge and highlight a specific summary comment by AUUG:

"[AUUG] ... would hope that the government would make the best technology choice at every juncture. Sometimes the best technology choice may indeed be a proprietary system. It may provide features, capabilities or some functionality that is only available with that system. However, AUUG feels that the government should seriously consider using open systems, particularly where equivalent functionality is available at a much lower cost and with all the benefits of open source software."

Regulation of .eu domain names

The registration process for the .eu domain names is due to commence later this year. Any individual who is resident within the EU, any undertaking having its registered office, central administration or principal place of business within the EU and any organisation established within the EU will be able to register .eu domain names.

The .eu domain names are not intended to replace the current national ccTLDs of EU Member States. However, they will provide users with the opportunity of having a pan-European identity for their websites and e-mail addresses. The European Commission is responsible for putting in place the necessary steps for the implementation of the .eu TLD. The European Registry for Internet Domains ("**EURID**"), a private sector, non-profit organisation, will be responsible for the day-to-day management and operation of the .eu domain. It is hoped that EURID will be ready to commence with the registration process in the second half of 2004. Certain restrictions will be enforced to avoid abusive or speculative registrations such as a sunrise period allowing those holding prior rights to a name to register it prior to the general registration process commencing. Furthermore, public bodies will also have the opportunity to register their names in advance of the general public.

(This article was supplied courtesy of Vanessa Shield, Linklaters IT & Communications, Intellectual Property News, Issue27, March 2004.)