

Bell Gully's regular review of current legal issues affecting the communications, technology and media sectors.

Open source software – a free lunch?

Like any other business activity, using open source software involves risks and costs, and you need to ensure that those risks and costs are considered, and weighed up against the perceived benefits.

Digital archiving – legal requirements

Storing information in electronic form can result in significant cost savings and allow more effective document management.

Hackers beware – the Crimes Amendment Act works

A recent case provides a good insight into the impact and workings of the new computer crime offences, established by the Act late last year.

Privacy impacts of e-government authentication reported

The New Zealand government has given the go ahead for the development of a "whole of government" G2P authentication scheme, including the establishment of a single stand-alone authentication agency with a minimum of information exchange and storage.

Need more information?

For more information on any of the cases, articles and features in CTM Update, please contact the author, or email Simon Martin at simon.martin@bellgully.com or call on 64 9 916 8972.

Open source software - a free lunch?

At this very moment, someone, somewhere within your organisation is probably using open source software. Maybe it's being used to run mission critical servers or to slot into a newly developed application.

"So what", you might say, "it's better than a free lunch - the relevant open source software is good enough, practically cost free and makes business sense." However, just like any other business activity, using open source software involves risks and costs. You should ensure that those risks and costs are considered, and weighed up against the perceived benefits, before deciding whether or not that person should be allowed to continue using the open source software.

This article highlights the potential benefits of using open source software, contrasts those benefits against the risks, and suggests strategies to mitigate those risks. If you have any queries or concerns about the legal risks of using open source software, please contact one of Bell Gully's [IT law specialists](#).

What is open source?

In brief, open source software is software and its "human readable" source code made available by developers:

- a. without charge (or with a minimal charge);
- b. under very permissive licence terms (allowing copying, modification and redistribution of the software and its source code); and
- c. generally on an "as is where is" basis.

However, conditions are often placed on redistribution of open source software, including requirements that any redistribution of the software and any modifications:

- a. be on the same terms as the licence from the original developer; and
- b. include the source code and documentation for the original software and the modifications.

Conditions similar to these are set out in the GNU Public Licence, which applies to the use and distribution of Linux, but there is a broad variety of open source licences containing variations on these conditions.

It may be that there is a sole developer of the open source software, but it is more common for the open source software to have been developed by a number of different developers (i.e., a "community" of developers).

Open source software can be contrasted with closed source or "proprietary" software, the developers of which closely protect the source code, only providing the machine readable object code to licensees that have:

- a. paid the relevant licence fee; and
- b. agreed to much more restrictive licence terms.



communications, technology and media update

May 2004

What are the benefits?

The following key benefits can be identified in relation to open source software:

1. *You've got the source code*

Access to the source code means that you can better understand how the software works and undertake "self-help" remedy of bugs or problems. You (or your development team) can also develop or modify the software to better suit your requirements.

2. *Quality and security*

Given that the source code is made available to a number of developers, peer review by "many eyes" means that open source software can be more robust and secure than proprietary software. That said, this does not guarantee robustness or security, and lesser known open source software is unlikely to have been subject to the same scrutiny as well known open source software such as Linux.

3. *You are not alone*

Most open source software has a "community" of developers that contribute to its development or improvement. This community, and the open exchange of ideas that it fosters, often reduces the need to "re-invent the wheel" when considering a particular development or problem in relation to an open source product.

4. *Control the life of the software*

You have greater control over the usable life of open source software, as you are not necessarily reliant on the supplier continuing with a support and maintenance program. In effect, you are better able to avoid becoming a "captured customer".

5. *Up-front costs are low*

The lack of a significant up-front licence fee means that the up-front costs are low. If your business is growing fast, the ability to scale the use of the software, without incurring additional licence fees, means that ongoing costs can also be lower than proprietary software.

So what about those risks?

The following key risks can be identified in relation to open source software:

1. *Your open source licence could be unilaterally changed or even terminated*

Your open source licence could be terminated unilaterally because it may not be an enforceable contract. When lawyers try and decide if an enforceable contract exists they generally look for the following key elements:

- a. an offer by one person to establish a contract;
- b. acceptance by another person of the establishment of the contract;
- c. consideration (comprising payment or a promise to do something);
- d. certainty of the subject matter of the contract and the parties to the contract; and



- e. a general intention to create a contract.

Looking at open source licences, the key elements of "acceptance" and "consideration" may not be present as:

- f. most open source licences do not require the payment of a fee to the licensor;
- g. the promises made under some open source licences to distribute modifications on specified terms need only be kept if the licensee actually makes modifications and decides to distribute them (i.e., the customer decides whether or not the promise applies); and
- h. the licensee does not really have the opportunity to accept or reject the licence terms or make that acceptance known in a tangible way.

As two of the key elements of a contract could be missing, it is unlikely that the legal foundation for open source licences is contract law.

Instead, the legal foundation for open source licences is seen to be copyright law, and a copyright licence can be amended or terminated at any time by the licensor giving notice to the licensee. As a result, there remains a risk that an open source licence could be changed or terminated unilaterally at any time by the developer.

That said, if the open source software was developed by a number of developers, and they have joint ownership of the copyright in the software, then they would all need to agree to the change or termination.

It may also be possible to claim that the developer should be prevented from terminating or changing the open source licence under the common law doctrine of estoppel. This doctrine prevents people from going back on representations that others have relied on to their detriment. However, in each case it would be necessary to establish such a representation was made, as well as reliance by the relevant user to their detriment.

2. *The software is supplied "as is where is"*

The risk of problems with open source software falls on the user. In general, no warranties are provided in relation to the performance or operation of open source software. As a result, you cannot turn to your supplier and seek damages for breach of warranty.

That said, it may be possible to argue that the exclusion of implied warranties and tortious claims in most open source licences doesn't work at law (on the basis that the licence is a copyright licence, not a contractual licence, and copyright law does not support such exclusions).

This might be a difficult argument to win though, as the licence terms provide good evidence that the user has voluntarily assumed the risk of use. In addition, the relevant licensor may not have pockets deep enough to justify legal action.

Lastly, by way of comparison, it should be remembered that most proprietary software is supplied on terms and conditions that limit the developer's liability as much as possible (unless the user had very strong bargaining power at the time of licensing).



3. *No two open source licences are the same*

More than 50 different open source licences are listed on the Open Source Initiative's [website](#). As a result, it is not possible to assume that the kinds of use, development and distribution that you are contemplating will automatically be permitted by the applicable licence.

The main risk that arises here is that your rights to redistribute might be fettered. As mentioned above, a number of open source licences require that if modifications are made to the software and distributed, then they must be distributed with the source code for the modifications, on the same terms as the original licence (i.e., at no or minimal cost).

This does not present problems if you merely intend to develop modifications for internal use. However, if you plan on providing the modifications to others you do business with, or selling them to customers, then a check of the licence may indicate that you need to think again, as you might have to provide them at no charge or let your competitors also have access to the modifications.

4. *Open source does not mean free*

Although the up-front costs of open source software may be minimal, it must be remembered that there are other costs involved in the use of software, particularly maintenance and support. In this regard, a total cost of ownership approach should be taken to open source software, considering not just the up front licence costs, but the costs of support and maintenance and scaling for future growth.

Even though the source code for an open source product will be available, you should budget for and retain technical staff skilled in its use, support and modification, or contract with service providers to obtain access to such services. This need has provided business opportunities for organisations that specialise in the support and modification of open source products.

Recent studies initiated by major IT companies are equivocal as to the total cost of ownership of major open source products. On one hand, studies initiated by organisations that have their own open source initiatives (including hardware and support providers) indicate lower total costs of ownership of open source software. On the other hand, studies initiated by organisations that don't have open source initiatives indicate that proprietary software has a lower total cost of ownership. In effect, it will be up to you to make a call about the total cost of ownership of the software for your enterprise.

5. *You don't get a third party IP indemnity*

Most suppliers of proprietary software will give their customers an indemnity in relation to the breach of third party intellectual property rights (although these tend to be limited as much as possible). Under the indemnity, if the customer is sued by a third party on the basis that the software breaches the third party's copyright (or other intellectual property rights such as a patents), then the supplier is required to pay the customer's costs and step in to run the defence of the claim.

Most proprietary software suppliers give such an indemnity as they have confidence in the integrity of their software development processes and have good patent protection, or can carry the risk of patent claims (being satisfied based on patent searches that this risk is minimal).

Such indemnities are generally unavailable in relation to open source software, as the supplier cannot have the same certainty regarding the integrity of the development process. The risks that arise as a result have been high-lighted in the recent claims by SCO Group against IBM regarding breach of SCO's rights in Unix source code.



communications, technology and media update

May 2004

Perhaps as a result of this claim, some commercial suppliers of open source software are starting to offer indemnities regarding breach of third party intellectual property rights (for example, the supplier of the JBoss application server).

How do I mitigate those risks?

The first step in mitigating the risks that arise is to establish an enterprise wide policy on the use of open source software, and make sure it is followed.

At one extreme, this policy could completely ban the use of open source software but this would be a knee-jerk reaction and may not prove effective (as people sometimes react to outright bans by ignoring them). Instead it may be better to allow the controlled use of open source software, for example, only allowing the use of software that has proven to be reliable and robust and that is not subject to outstanding intellectual property claims.

Other risk mitigation steps to take include:

- a. documenting exactly what you want to do with the open source software;
- b. getting the licence terms checked by your legal team or one of Bell Gully's IT law specialists and making sure they are consistent with your intended use;
- c. checking out the supplier - you want to know that you are dealing with a reputable entity;
- d. checking out the background to the open source software - are there reports of poor performance or security problems, or does it have a good reputation;
- e. establishing whether there are any existing or threatened intellectual property claims in respect of the open source software; and
- f. outlining a reasonable exit strategy, so that you are not excessively exposed if you have to stop using the open source software because of third party intellectual property claims, or termination or amendment of the licence.

Lastly, if you have sufficient bargaining power and you are obtaining the software from a significant supplier, you could also ask the supplier to take on the risk of third party intellectual property claims through an indemnity.

Jeremy Salmond

Senior Associate

Tel: 64 4 915 6951

Email: jeremy.salmond@bellgully.com

Digital archiving – legal requirements

To many business managers, the sheer volume of paperwork involved in operating a business today might seem to threaten to bury the company under a landslide of accounting records, contracts and minutes of long forgotten meetings.

The management of a company's information stored in paper form can be an expensive administrative headache. Fortunately, the new Electronic Transactions Act (ETA) and recent improvements in information technology mean that electronic storage of important documents is now a viable and efficient method for companies to manage their information.

Storing information in electronic form and discarding original hard copies can result in significant cost savings and, potentially, could also allow more effective contract management and referencing of historical records.

There are two principal reasons why a company may retain information. First, it may be required by law to do so. Second, the company may wish to retain information as a record of its transactions, commitments and business generally. This article will briefly discuss the legal implications of electronic storage of information for each of these reasons, before setting out some very general guidelines for digital archiving.

Electronic storage and a company's statutory obligations

What statutes might apply?

Companies are required to retain information under a number of statutes. The two most common are the Income Tax Act and the Companies Act. However, when considering what records must be retained, a company should consider all of the statutes, rules and regulations governing that company's particular field of business as these statutes may impose specific requirements for storage of information. For example, the Medicines Act requires manufacturers of pharmaceuticals to retain information regarding the quality and testing of any medicines they distribute.

The ETA provides guidelines for companies wishing to retain electronically information that they are required to store. However, statutory or regulatory bodies such as the Inland Revenue Department (IRD) may also issue their own guidelines on electronic record retention. For example, the IRD has released an exposure draft setting out a number of requirements for retention of business records for tax purposes.

Storing paper based records in electronic form

Under the ETA, a legal requirement to retain information that is in non-electronic (i.e. paper) form is satisfied by retaining an electronic form of the information provided that:

1. the electronic form can reliably maintain the integrity of the information; and
2. the information can easily be accessed for subsequent reference.

To satisfy the first requirement, integrity of the information will be retained only if the information has remained complete and unchanged in any material way (the implementation of an audit trail as suggested below will help prove this requirement).



communications, technology and media update

May 2004

The second requirement will be satisfied if the information can be readily accessed using the information holder's equipment, or with equipment that could be easily obtained from a third party.

Storing electronic based records

Under the ETA, information originating in electronic form can be retained in that electronic form provided that its storage meets the standards of integrity and accessibility outlined above.

Otherwise, such electronic information can be converted into and stored as a hard copy so long as the information is not altered in the conversion.

Storing electronic communications

Where information that must be retained is in the form an electronic communication (e.g. an email), the ETA's standard requirements for electronic storage of information apply. In addition, however, further information relating to the origin, destination and time the communication was sent and received must also be retained. This additional information must also be retained even if the communication is stored in paper form.

Provision of electronic records

Obviously, at some point stored records will need to be reviewed or disclosed. The ETA provides guidance on when a company may perform its disclosure obligations by providing information in electronic form (e.g. by way of an email or on a disk).

A company may disclose data in electronic form if three conditions are met. These are that: the method used to supply the data reliably assures its integrity; the information supplied is readily accessible; and the person requesting the information consents to receiving the information in electronic form. If these criteria are not met then information will need to be provided in more traditional paper-based form.

Electronic storage of a company's non-statutory information

The ETA sets out how information required to be retained by statute may be validly stored. However, chances are that a business will want to archive much more information than merely its statutory requirements.

The main driver will be records of agreements reached so that should a dispute arise there is evidence of what was agreed (this may take the form of a formal contract, correspondence and/or business records).

There is little to be gained from retaining business records, contracts and correspondence if that information cannot be relied on should a dispute arise. Accordingly, it is important to look at the court's rules of evidence in determining what steps should be taken to ensure that information stored electronically can be relied on in a dispute.

The Evidence Amendment Act defines a document as including "Any information stored by means of any...computer". Therefore, the evidence rules governing the admissibility of documents will be relevant to information in electronic form. The rules of evidence that may apply in determining the admissibility of electronic information are:

- (a) Hearsay
- (b) The best evidence rule
- (c) Authentication

© Bell Gully 2003. All rights reserved.

Disclaimer: This publication is necessarily brief and general in nature. You should seek professional advice before taking any further action in relation to the matters dealt with in this publication.



communications, technology and media update

May 2004

"*Hearsay*" is evidence of a fact given by a person who does not have first-hand knowledge of the fact. Hearsay evidence is usually inadmissible in a court because it is considered to be second-hand evidence and therefore unreliable. This rule may present problems for the admissibility of electronic information.

For example, where data is entered into a computer system by a person who does not have first-hand knowledge of the data's derivation or accuracy, that person cannot present the data as evidence in court.

However, there is an exception to the hearsay rule in respect of "business records" (as defined in the Evidence Amendment Act). Briefly, a business record is a document made from information supplied by a person with first-hand knowledge of the information where this document is made pursuant to a duty or in the course of business.

Where a document falls into this category, it may be admitted as evidence in court without the need for the person recording the information to testify as to the document's accuracy or derivation.

"*Best Evidence*" - the best evidence rule requires that a party to court proceedings produces the best evidence available. Traditionally, this rule has meant that where documentary evidence is relied on only the original document was admissible. The rationale for the rule was that any copied document may not be entirely accurate and copying errors could affect the content of the document.

Although the best evidence remains an original document, digitally scanned copies of the document are now admissible in court. This position recognises that copies can now be made inexpensively and accurately, with minimal potential for error or inaccuracy in the copy.

"*Authentication*" - the authenticity of a document must be established before that document will be admissible as evidence. Documents stored electronically are inherently more vulnerable to either accidental or intentional change than paper documents. For example, information stored electronically may be at risk of system failures, software corruption and unauthorised access (both internal and external).

Therefore, before electronically stored documents are produced as evidence in place of the original, additional evidence of the reliability of the copying and storage processes may also be required. (Some suggestions on implementing a reliable conversion and storage process are set out below).

Any business using or intending to implement a system for electronic storage of documents should consider their storage system and the process for capturing the relevant documents in light of these three rules of evidence. Otherwise, a business faces the risk that it will not be able to rely on important documents it stores in electronic form.

How long should information be stored?

There are a number of factors to take into account when deciding how long information should be retained.

We have already referred to the specific requirements for electronic storage of business records under the Income Tax Act. This Act also provides that all tax records must be kept for a minimum period of seven years. Obviously, business records stored electronically should be stored for at least this period or any longer period required by any other statute governing a company's business.

However, there are many situations where it would be prudent to retain information for significantly longer than seven years. For litigation purposes, there is generally a limitation period of six years from the date on which a cause of action arises (although this period can vary for different types of claims). That is, claims may be filed in court up to six years after the occurrence of the act resulting in a claim.



communications, technology and media update

May 2004

If this act was a breach of a ten-year contract in its tenth year, then the limitation period for litigation would not expire for a further six years, and the contract document might be required more than 16 years after it was created. Other documents related to the contract may also remain relevant for a similar period of time.

On a practical level, it would be extremely expensive to store all business information for an indefinite period of time. Therefore, in determining how long to retain its documents, a business should ensure that it complies with any statutory requirements and after this weigh the costs of storing a document for a certain period against the risk that such a document will be required outside of the period and the likely cost if that document were not available.

When should information not be stored?

While most statutes focus on a requirement to retain information for a certain period, there are some statutes that prohibit the storage of information for longer than is necessary. The most common example is the Privacy Act which provides that if information is held about identifiable individuals, under the Privacy Act this information should not be retained for longer than is necessary for the purposes it was collected for. Again, a company should consider what statutes govern its business and what requirements these have on ceasing to store information.

Basic guidelines for digital archiving

The ETA requires that where information is stored electronically the method of storage must preserve the integrity of the information. In a similar fashion, the court rules of evidence require that an electronic document must be authenticated as true and accurate before it can be relied on. The following suggestions provide a basic overview of how electronic archiving can be managed to preserve the integrity of information and make authentication of that information more simple.

- A process for capturing information on when and how information was copied, who authored the original document, who copied the document and how the information will be stored should be established. This will aid in authentication of any information produced in court.
- Strict controls and rules should be established covering the generation of documents, scanning of documents, storage of documents and retrieval of documents. Compliance with these controls should be monitored.
- Access to records should be controlled and tracked by use of an identification process – for example, use of individual access codes or digital signatures. This will aid in establishing reliability of information if it is ever brought into question.
- Information should be stored on a non-erasable optical disc to ensure that information cannot be altered or deleted. If this is not possible then 'write privileges' to a storage database should be restricted.
- Records should be backed up and copies should be stored off site to prevent loss of records in the event of fire or system-wide equipment failure.
- Technology used to store information should be capable of storing the information for the designated life time of the document. If data degradation is a risk the data should be recopied before this occurs and information should be retained to provide evidence that the recopying did not prejudice the reliability of the information.



communications, technology and media update

May 2004

- Information should be managed over time to prevent stored data becoming inaccessible as a result of technology becoming obsolete. For example, if information is stored on a document retrieval system that is based on one platform and the business moves to another platform, provision should be made to ensure that the stored data can still be accessed.

The bottom line

- Significant cost and administrative advantages can be gained by electronic storage of data.
- Certain statutes require businesses to retain specific information. If certain guidelines are adhered to (especially those of the Electronic Transactions Act), this information can be stored and disclosed in electronic form.
- Business information stored electronically can be relied on in a dispute provided that the information complies with the court rules for admissibility of evidence.
- Technological, process and practical issues should be considered in establishing and maintaining an electronic information storage system.

Simon Martin

Partner

Tel: 64 9 916 8972

Email: simon.martin@bellgully.com

A version of this article was first published in *IT Brief*.

Hackers beware – the Crimes Amendment Act works

*You might have noticed in the papers that a Dunedin man recently pleaded guilty to charges of hacking into a US-based e-commerce operator's systems. This case, involving damages claims of US\$458,000, is a timely reminder of the importance of the "anti-hacking" provisions established by the Crimes Amendment Act 2003 (**the Amendment Act**).*

The attacks in question occurred late last year, causing severe disruption to electronic stores run by Oregon-based "BuyMusicHere". The attacks reduced the operation of the "BuyMusicHere" database in Oregon to a virtual crawl. Co-operation between the New Zealand police and US authorities led to the prosecution. The hacker (who has name suppression) pleaded guilty to three charges of damaging a computer system and unlawful access (new "computer crimes" under sections 249 and 250 of the Crimes Act).

This case provides a good insight into the impact and workings of the new computer crimes, established by the Amendment Act late last year. Before the passing of the Amendment Act, New Zealand was one of the few Western countries without specific computer offences. Under our old law, hackers could only be convicted under general theft and criminal damage provisions of the Crimes Act (which were not always applicable to hacking activity). Were it not for the Amendment Act, the Dunedin hacker may have remained unpunished.

The Dunedin hacking case also clarified that the new computer crimes in the Amendment Act extend to cover damage caused from New Zealand, but which occurs on computer systems overseas.

So what changes did the Amendment Act make?

Illegal access

Section 249 of the amended Crimes Act makes it illegal to access a computer system for a dishonest purpose.

In order to be convicted under this section, an offender must access a computer system with the intent to obtain property, privilege, service, pecuniary advantage, benefit, or valuable consideration or cause loss to a person. An offender will be caught under this section whether or not they actually gain any such benefits or cause loss, provided that it was their intention to do so.

It is worth noting that if someone accesses a system, for example during the course of their employment, and believes that they are entitled or authorised to obtain a benefit, then to do so may not breach section 249.

Unauthorised use of data

Section 250 of the amended Crimes Act makes it illegal to intentionally or recklessly damage a computer system or intercept, access, use or damage data held on computers without authorisation. This could include an attempt to put a website out of action (i.e., a denial of service attack) or interfering with someone else's data. This offence has a maximum sentence of seven years' jail, increasing to ten years if the offender knows or ought to know that damage to life is likely to result.

Debate about this section has largely centred around the meaning of "authorisation" and the effect this has on the application of this section. It has been suggested that the inclusion of this word creates a loophole in the Act, which allows employees (who are authorised to access the computer system) to intercept, access, use or damage data held on the computer without being caught by the provisions of the Act. However, whether this in fact happens will depend on the interpretation that the courts give to the word "authorisation".

The courts may decide that a person is "authorised" for the purposes of the Act if they have authority to access a particular part of the computer system. If this interpretation is adopted then such a person cannot be liable under this section. However, such an interpretation would not appear to be sensible or consistent with the purpose of the legislation. Instead, it seems more likely that the courts will adopt a pragmatic approach and hold that a person is "authorised" only for specific purposes and that action outside those specific purposes, such as deleting a file from a computer for a malicious reason, is not authorised behaviour.

Unauthorised access

The Amendment Act also makes simply accessing a computer system without authorisation illegal. This means that "pure hacking", or hacking into a computer system without gaining a benefit or causing harm, is now illegal. The Amendment Act imposes a maximum penalty for "pure hacking" of two years' imprisonment.

Concerns have been raised in relation to this provision. These include the fact that penalties for the computer-specific offence are far more severe than those for an equivalent offence in the "real world". Critics of the Act see pure hacking as a minor offence and think that it is occasionally helpful in that it alerts organisations to weaknesses in their security. Arguments that "pure hacking" are beneficial and should not be illegal seem to avoid the fact that hackers are deliberately breaking into a system they are not authorised to enter.

Hacking Tools Banned

The new section 251 has also proved to be controversial. It makes it illegal to sell, distribute or possess computer hacking programmes in New Zealand.

It has been suggested that this provision:

- overlooks the importance of educational websites and other information that deals with hacking; and
- may prevent individuals or organisations learning more about hacking programmes in order to protect against them.

On the face of it, such criticisms may be justified. Whether or not the Amendment Act will actually have this effect will only become clear through the passage of time. In this regard, "good" users of such information may have to rely (tentatively) on the police's discretion whether or not to prosecute a particular case.

Powers of interception

The Amendment Act also changed the police interception warrant provisions of the Crimes Act. Previously, law enforcement agencies acting under interception warrants could only intercept oral communications. The Amendment Act broadens law enforcement agencies' powers under interception warrants and allows them to intercept written communications such as emails, facsimiles and text messages. This is required as the old ban on the use of listening devices is extended by the Amendment Act to cover any communications interception device.



communications, technology and media update

May 2004

An exception to the new ban on the use of interception devices is also provided for ISP's and communications companies using such devices in limited circumstances for maintenance purposes. The Amendment Act makes it clear that a law enforcement agency is not committing an offence if it has a legal basis, such as a search warrant, for accessing a computer.

A healthy level of debate about infringement of privacy occurred when the new interception powers were tabled. The Amendment Act goes some way towards addressing such "privacy" concerns by requiring police to specify the person, place, specific electronic address, phone number or similar facility relevant when applying for an interception warrant. However, a number of people remain concerned about the interception powers. Whether these concerns are warranted will probably only be clarified with the passage of time.

Jeremy Salmond

Senior Associate

Tel: 64 4 915 6951

Email: jeremy.salmond@bellgully.com

Privacy impacts of e-government authentication reported

In June 2003, the New Zealand government gave the go ahead for the development of a "whole of government" G2P authentication scheme, involving the establishment of a single stand-alone authentication agency with a minimum of information exchange and storage.

By adopting this approach, the basic identity information supplied by the individual and verified by the authentication agency is kept separate from more privacy sensitive service information held by the agency that actually provides the government service.

The information interchange between the authentication agency and the service agency is limited to the release of identity data (name or names/gender/ date and place of birth) as authorised by the relevant individual using a password or other key (such as a digital certificate) with which his or her identity credentials have been previously associated.

As part of the on-going design work for the scheme, government commissioned a privacy impact assessment ("PIA") by outside consultants. The consultants' report has now been released publicly.

The report is generally supportive of scheme's direction, which:

- recognises that not all online government services require authentication;
- is not based on a national ID card;
- will not require a uniform PKI-based authentication solution; and
- provides for authentication (verifying identity) to be handled independently from authorisation (access to services).

However, there are other features of the scheme on which "red flags" have been raised.

For example, one of the scheme's design assumptions is that the public should be able to choose whether or not to access services that require online authentication (the "opt-in" principle). The report questions whether this objective can be maintained over time.

It suggests that in order to make the scheme financially viable, government will be tempted to proactively promote the online alternative by offering the public incentives to convert, and by making offline service delivery channels more difficult to access.

In addition, the report predicts that one large category of initial users will be those conducting online transactions for business purposes. Such people are likely to be required by their employers to obtain ID credentials from the authentication agency in order to carry out their job. The report notes that the proposed authentication model makes no provision for the issuance of ID credentials based on organisational roles, even though in many B2G transactions service agencies have no need to actually identify individuals.



communications, technology and media update

May 2004

Another issue raised by the report, concerns the ongoing use of the photograph that the individual is required to provide when he or she applies to the authentication agency for the issue of ID credentials. The photograph is to be required to ensure that one individual does not try to register more than one identity.

The current design assumes that the photographic image and its associated biometric will be retained by the authentication agency. The report questions the need for the retention of this kind of information, especially given the risk of false negatives using face recognition technology and the fact that ID credentials (with the resubmission of photographs and other identifier information) will have to be renewed on a periodic basis. The authors of the report also express concern on the possibility of use of this kind of information by service agencies over time.

The report also:

- notes that the design needs to include how possible failures in the system will be dealt with, coupled with an acceptable set of rights and remedies available to those unfortunate individuals who are the subject of operational errors concerning their identity;
- calls on government to clarify the application of various aspects of New Zealand's Privacy Act to the scheme particularly around the use of the ID credential as a unique identifier and the control and regulation of authorised data matching operations between government departments;
- stresses the need for a comprehensive and continuing security and risk assessment (on data quality and other matters) to address the many security issues affecting the scheme that remain unresolved.

These issues and others that are canvassed in the report could, the authors say, result in a system that evolves into a kind of national population register, with all the potential that such a system has for secondary uses of information or subsequent extensions (including the adoption of a national identity card system, a development currently rejected by government.)

It is stated that this impression will only be managed properly by strongly and deeply entrenched legislative safeguards. The report makes a number of detailed recommendations as to the kind of privacy enhancing measures that should be included in the statute that sets up the authentication agency.

Stephen Revill

Partner

Tel: 64 4 915 6997

Email: stephen.revill@bellgully.com