

Submission to the Inquiry into the Privacy Amendment (Enhancing Privacy Protection) Bill 2012

The [Privacy Amendment Bill 2012](#) is written within the constraints of the existing practices for collection and use of personal data. The writers of the legislation have tried to be technology neutral. Unfortunately it is difficult to devise policy rules without making assumptions on the technology used to operate the system. This is evident in the [explanatory memorandum](#) and in the volume of legislation to protect privacy in the reporting of credit history. Most of the changes to legislation are required because of the technology currently used to implement the reporting of credit history.

Privacy issues arise when personal data is stored and shared between organisations and persons. In particular two technologies influence how the system operates and hence the legislation is not technology neutral. These technologies are:

1. For some purposes it is assumed that the most efficient way to share data is to collect copies of data from disparate groups and store them in large databases. Examples are files kept by credit bureaus, and files kept by the Tax Office.
2. Often it is impractical to create a single data base of data but the data still needs to be shared. It is assumed that the most efficient method of sharing is to give each individual a unique identifier to be used across the different databases. An example is the current ehealth initiative and attempts by the government to introduce a common govID.

In today's connected world with rapid communications and powerful computers there is a more efficient technology to share and combine data. This can thought of as "just in time sharing". Data is not shared or collated until there is a need to do so. This can be achieved by providing a means for an individual's data to be shared at the time it is needed - and not before. The two technologies described in 1 and 2 above combine ALL data even though it may never need to be combined.

A "just in time" technology can be implemented easily and simply by providing a mechanism for an individual to access their own data at the time it is stored and informing the individual when personal data is accessed by a third party.

To make it possible for a "just in time" technology to operate effectively the legislation can include two extra ideas.

1. Whenever personal data is stored by an organisation that follows the National Privacy Principles (NPP) the individual must be informed and given access to the data stored.
2. Whenever stored personal data is accessed by a party other than the NPP the individual must be informed that the access has occurred, by whom, and what data has been accessed.

Informed means that the person has the right to know and can access the information if they so desire. It does not mean they are notified immediately.

These additions do not conflict with the proposed amendments. Those cases where a person is not permitted to be told what information is stored are already covered by the legislation and those sections can override 1 and 2.

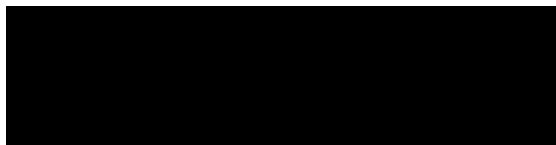
These additions reinforce existing privacy principles on right of access and make it more likely that errors in data storage will be detected.

There is no need to change existing systems and the rules need only apply to new systems and to changes to existing systems.

Implementation is inexpensive and can be made “automatic” and implemented for a very low cost. Implementation is inexpensive because the NPP has obtained permission from the person before the data is stored and so is in contact with them. The NPP uses the same communications channel to tell the person how to access the stored data. When a third party accesses the data the NPP uses the same communications channel to tell the person that their data has been accessed.

The additions will be shown to dramatically reduce the cost of compliance. It will dramatically reduce the cost of operating information systems holding personal data whether data is collected in databases, or data is federated using common identifiers, or whether “just in time” collation of data occurs or whether some unthought of innovation occurs.

It is likely that there will be a wholesale conversion of existing systems to use the new technology because it results in very efficient, very private systems. This happens because compliance of most of the privacy principles are automatically achieved if “just in time” technology is used.



Kevin Cox
12th July 2012