What is cloud computing?

Cloud computing has the potential to transform the way individual consumers and small businesses store and use data, potentially saving time, money and effort. However, cloud computing involves risks for consumers that must be carefully managed.

Cloud computing lets you do tasks online that were once offline. Cloud computing can be a method of saving and storing your information. Instead of storing information on a local machine or network (e.g. on your hard drive) cloud computing lets you store your information (or data) remotely, on servers that might be in another building, city or even country.

Cloud computing can also be a way of using software or services. For example, you can use word processing software online, like Google docs, without ever having to download the specific software to your computer. You may already be using a cloud computing service like Hotmail or other web-based email services.

Cloud computing can contain risks as it requires users to relinquish absolute control of their data, trusting a service provider to protect documents they once controlled directly. Think of it this way, previously small businesses would keep financial records and sensitive documents in a safe place in the office, maybe in a filing cabinet with a lock. The business owner was responsible for keeping these documents secure – he or she would know how many people had copies of the key and would be aware if someone broke in. With cloud computing, the documents that were once stored in the office are now stored externally and are managed and protected by another company.

Data or services in the cloud are only accessible via an internet connection. This means that if you are thinking about using a cloud service you will need a fast, reliable internet connection. You will also need to think about additional costs for increased data uploads and downloads.

ACCAN position statement: What consumers need from cloud computing.

1. Access

Like any online services, cloud computing should be accessible to all consumers. Companies should use the WCAG 2.0 guidelines to ensure that people with disability are able to navigate all aspects of the service. Cloud computing has the potential to create more accessible services for all Australians. This potential should be actively explored by government and industry groups.

2. Interoperability

It should be easy to transfer data from one service to another. Consumers must be able to alter, transfer or completely delete their data on request; this must include cached and backed-up data controlled by the service provider. Services should be compatible with multiple operating systems.

3. Ownership

Data uploaded to cloud services must remain the property of the user. Services should not use or allow secondary parties to use data without specific opt-in consent from the user.

4. Privacy

Services should respect a user's right to privacy and follow international best practice in data protection. At a minimum, providers must comply with data protection requirements under Australian law including the Australian National Privacy Principles.

5. Redress

Companies must actively inform consumers about how to make a complaint or ask a question; this process must be easy to use. Providers should offer appropriate compensation in cases when data is lost or privacy is breached.

Where users are accused of breaching terms of use, they must be informed of specific allegations and given the right to appeal. Before termination of any service due to a breach of terms of use, unless the user is charged with a crime, users must be given the opportunity to access and download their data.

Governments and regulators should ensure consumers have access to a free and easy-to-use external dispute resolution system for cloud services. All cloud services sold to Australian consumers, regardless of jurisdiction, should be subject to Australian redress mechanisms.

6. Simplicity

Services should be presented in a manner that is easy to understand and allows consumers to compare similar products. Companies should offer a summary of important terms and conditions prior to purchase.

7. Security

Services must maintain sufficient security measures to protect information stored within and transferred between the user and the cloud. Compliance with best practice security standards should be monitored through independent auditing. Users should be provided with clear information about measures taken to protect the security of data at flight and at rest. Services should inform users about the best ways to protect information requiring different levels of security.

Service providers must make adequate back-up arrangements to avoid data loss. This should include back-up arrangements across different physical locations in case of a natural disaster or power failure.

Users should be notified in the event that their information is accessed, or is reasonably suspected to have been accessed, by an unauthorised party. The notification should include, at a minimum, a description of the breach, the time at which the breach occurred, the data that is likely to have been accessed in the breach, and procedures for redress if a security breach occurs.

8. Transparency

As a matter of best practice, cloud services provided to Australian consumers should be subject to Australian laws including laws relating to data protection, consumer protection, contracts and law enforcement.

Service providers should disclose the national jurisdiction or jurisdictions that apply to processing and data storage services. If a jurisdiction outside of Australia applies, the service provider should provide a summary of any relevant differences between Australian law and the applicable jurisdiction or jurisdictions.

Where a choice of jurisdiction is available, this should be offered to users. When a provider proposes to change the jurisdiction, users should be informed prior to the change and provided with an option to cease the service at no cost.