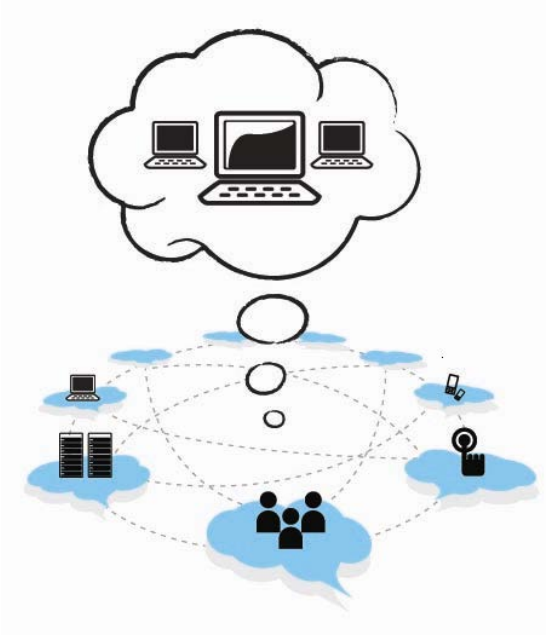
Commissariat à la protection de la vie privée du Canada
Office of the Privacy Commissioner of Canada

Fiche d'information | Fact Sheet

Introduction to Cloud Computing

When you store your photos online instead of on your home computer, or use webmail or a social networking site, you are using a "cloud computing" service. If you are an organization, and you want to use, for example, an online invoicing service instead of updating the in-house one you have been using for many years, that online invoicing service is a "cloud computing" service.



Cloud computing refers to the delivery of computing resources over the Internet. Instead of keeping data on your own hard drive or updating applications for your needs, you use a service over the Internet, at another location, to store your information or use its applications. Doing so may give rise to certain privacy implications.

For that reason the Office of the Privacy Commissioner of Canada (OPC) has prepared some responses to Frequently Asked Questions (FAQs). We have also developed a Fact Sheet that provides detailed information on cloud computing and the privacy challenges it presents.

Cloud Computing

Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications.

30, rue Victoria | 30 Victoria Street
Gatineau (Québec) K1A 1H3
Sans frais/Toll free 1-800-282-1376 Tél./Tel: 819-994-5444 Téléc./Fax: 819-994-5424 www.priv.gc.ca

The following definition of cloud computing has been developed by the U.S. National Institute of Standards and Technology (NIST):

> *Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.*[1]

Characteristics

The characteristics of cloud computing include on-demand self service, broad network access, resource pooling, rapid elasticity and measured service. On-demand self service means that customers (usually organizations) can request and manage their own computing resources. Broad network access allows services to be offered over the Internet or private networks. Pooled resources means that customers draw from a pool of computing resources, usually in remote data centres. Services can be scaled larger or smaller; and use of a service is measured and customers are billed accordingly.

Service models

The cloud computing service models are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). In a Software as a Service model, a pre-made application, along with any required software, operating system, hardware, and network are provided. In PaaS, an operating system, hardware, and network are provided, and the customer installs or develops its own software and applications. The IaaS model provides just the hardware and network; the customer installs or develops its own operating systems, software and applications.

Deployment of cloud services:

Cloud services are typically made available via a private cloud, community cloud, public cloud or hybrid cloud.

Generally speaking, services provided by a **public cloud** are offered over the Internet and are owned and operated by a cloud provider. Some examples include services aimed at the general public, such as online photo storage services, e-mail services, or social networking sites. However, services for enterprises can also be offered in a public cloud.

In a **private cloud**, the cloud infrastructure is operated solely for a specific organization, and is managed by the organization or a third party.

In a **community cloud**, the service is shared by several organizations and made available only to those groups. The infrastructure may be owned and operated by the organizations or by a cloud service provider.

---

[1] NIST cloud definition, version 15 http://csrc.nist.gov/groups/SNS/cloud-computing/

A **hybrid cloud** is a combination of different methods of resource pooling (for example, combining public and community clouds).

Why cloud services are popular

Cloud services are popular because they can reduce the cost and complexity of owning and operating computers and networks. Since cloud users do not have to invest in information technology infrastructure, purchase hardware, or buy software licences, the benefits are low up-front costs, rapid return on investment, rapid deployment, customization, flexible use, and solutions that can make use of new innovations. In addition, cloud providers that have specialized in a particular area (such as e-mail) can bring advanced services that a single company might not be able to afford or develop.

Some other benefits to users include scalability, reliability, and efficiency. Scalability means that cloud computing offers unlimited processing and storage capacity. The cloud is reliable in that it enables access to applications and documents anywhere in the world via the Internet. Cloud computing is often considered efficient because it allows organizations to free up resources to focus on innovation and product development.

Another potential benefit is that personal information may be better protected in the cloud. Specifically, cloud computing may improve efforts to build privacy protection into technology from the start and the use of better security mechanisms. Cloud computing will enable more flexible IT acquisition and improvements, which may permit adjustments to procedures based on the sensitivity of the data. Widespread use of the cloud may also encourage open standards for cloud computing that will establish baseline data security features common across different services and providers. Cloud computing may also allow for better audit trails. In addition, information in the cloud is not as easily lost (when compared to the paper documents or hard drives, for example).

Potential privacy risks

While there are benefits, there are privacy and security concerns too. Data is travelling over the Internet and is stored in remote locations. In addition, cloud providers often serve multiple customers simultaneously. All of this may raise the scale of exposure to possible breaches, both accidental and deliberate.

Concerns have been raised by many that cloud computing may lead to “function creep” — uses of data by cloud providers that were not anticipated when the information was originally collected and for which consent has typically not been obtained. Given how inexpensive it is to keep data, there is little incentive to remove the information from the cloud and more reasons to find other things to do with it.

Security issues, the need to segregate data when dealing with providers that serve multiple customers, potential secondary uses of the data—these are areas that organizations should keep in mind when considering a cloud provider and when negotiating contracts or reviewing terms of service with a cloud provider. Given that the organization transferring this information to the provider is ultimately accountable for its protection, it needs to ensure that the personal information is appropriate handled.

Privacy is not a barrier but it must be taken into consideration

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) does not prevent an organization from transferring personal information to an organization in another jurisdiction for processing.

However, PIPEDA establishes rules governing those transfers — particularly with respect to obtaining consent for the collection, use and disclosure of personal information, securing the data, and ensuring accountability for the information and transparency in terms of practices.

For more information on the views of the Office of the Privacy Commissioner of Canada with respect to outsourcing of personal data processing across borders, please see our *Guidelines for Processing Personal Data Across Borders*. These considerations apply whether moving data in the cloud or otherwise.

It is important to note that many non-Canadian based cloud providers may also be subject to PIPEDA. To the extent that a cloud provider has a real and substantial connection to Canada, and collects, uses or discloses personal information in the course of a commercial activity, the provider is expected to protect personal information, in keeping with PIPEDA.

Conclusion

Cloud computing offers benefits for organizations and individuals. There are also privacy and security concerns. If you are considering a cloud service, you should think about how your personal information, and that of your customers, can best be protected. Carefully review the terms of service or contracts, and challenge the provider to meet your needs.

For more information on cloud computing, see:

Reaching for the Clouds

The Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing

Guidelines for Processing Personal Data Across Borders

Frequently Asked Questions

What is cloud computing?

Simply put, cloud computing is the delivery of computing services over the Internet. Whether they realize it or not, many people use cloud computing services for their own personal needs. For example, many people use social networking sites or webmail, and these are cloud services. Photographs that people once kept on their own computers are now being stored on servers owned by third parties. These are also examples of cloud services.

Cloud services are popular because people can access their e-mail, social networking site or photo service from anywhere in the world, at any time, at minimal or no charge. Some cloud providers may, however, use the personal information of users for advertising purposes or to learn more about the users for other reasons. The Office of the Privacy Commissioner of Canada (OPC) has been critical of some of these practices, largely because they occur without individuals fully realizing how their personal information is being used "in the cloud." Individuals should pay careful

attention to whether and how the cloud company protects their personal information. Users should also protect their own personal information by using any privacy settings that the service may offer.

Can cloud computing affect privacy?

When it comes to cloud computing, the security and privacy of personal information is extremely important. Given that personal information is being turned over to another organization, often in another country, it is vital to ensure that the information is safe and that only the people who need to access it are able to do so. There is the risk that personal information sent to a cloud provider might be kept indefinitely or used for other purposes. Such information could also be accessed by government agencies, domestic or foreign (if the cloud provider retains the information outside of Canada).

For businesses that are considering using a cloud service, it is important to understand the security and privacy policies and practices of the provider. The terms of service that govern the relationship with the provider sometimes allow for rather liberal usage and retention practices.

Which party is accountable for personal information? The business that collects it from individuals or the cloud provider?

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) does not prohibit cloud computing, even when the cloud provider is in another country. Under PIPEDA, organizations must ensure that they collect personal information for appropriate purposes and that these purposes be made clear to individuals; they obtain consent; they limit collection of personal information to those purposes; they protect the information; and that they be transparent about their privacy practices.

PIPEDA also requires that when an organization transfers personal information to a third-party for processing, it remains accountable for that information. It must use contractual or other means to ensure that the personal information transferred to the third party is appropriately protected. Therefore, an organization that is considering using a cloud service remains accountable for the personal information that it

transfers to the cloud service, and it must ensure that the personal information remain protected in the hands of that cloud service provider. Organizations need to carefully review the terms of service of the cloud provider and ensure that the personal information it entrusts to it will be treated in a manner consistent with PIPEDA. For more information on transferring of personal information to third parties, please see our *Guidelines for Processing Personal Data Across Borders*.

Why are organizations interested in cloud computing?

Cloud computing can significantly reduce the cost and complexity of owning and operating computers and networks. If an organization uses a cloud provider, it does not need to spend money on information technology infrastructure, or buy hardware or software licences. Cloud services can often be customized and flexible to use, and providers can offer advanced services that an individual company might not have the money or expertise to develop.

I've heard that cloud computing may improve privacy protection. Is this true?

For businesses that are considering using a cloud service, cloud computing could offer better protection of personal information compared with current security and privacy practices. Through economies of scale, large cloud providers may be able to use better security technologies than individuals or small companies can, and have better backup and disaster-recovery capabilities. Cloud providers may also be motivated to build privacy protections into new technology, and to support better audit trails.

On the other hand, while cloud computing may not increase the risk that personal information will be misused or improperly exposed, it could increase the *scale* of exposure. The aggregation of data in a cloud provider can make that data very attractive to cybercriminals, for example. Moreover, given how inexpensive it is to keep data in the cloud, there may be a tendency to retain it indefinitely, thereby increasing the risk of breaches.

For more information, please see Cloud Computing.