CANADIAN PERSPECTIVES

on Cloud Computing and Consumers

Final Report of the Research Project
Presented to Industry Canada's
Office of Consumer Affairs

union des consommateurs

June 2011

Report published by:

union des consommateurs

6226 Saint-Hubert Street
Montreal, Quebec H2S 2M2

Telephone: 514-521-6820
Toll free: 1 888 521-6820
Fax: 514-521-0736

info@uniondesconsommateurs.ca
www.uniondesconsommateurs.ca

Union des consommateurs members:
Abitibi-Témiscamingue ACEF
Amiante – Beauce – Etchemins ACEF
Montreal East ACEF
Île-Jésus ACEF
Lanaudière ACEF
Estrie ACEF
Grand-Portage ACEF
Montérégie East ACEF
Montreal North ACEF
Quebec City South Shore ACEF
ACQC
Individual members

Written by
- Union des consommateurs

Research
- Anthony Hémond

Editorial management
- Marcel Boucher

ISBN 978-2-923405-48-3

Union des consommateurs is a member of the International Consumer Organization (ICO), a federation of 234 members from 113 countries.

The masculine is used generically in this report.

Union des consommateurs wishes to thank Industry Canada for helping to fund this research project. The views expressed in this report are not necessarily those of Industry Canada or the Government of Canada.

TABLE OF CONTENTS

UNION DES CONSOMMATEURS, *Strength through Networking*

Union des consommateurs is a non-profit organization whose membership is comprised of several ACEFs (*Associations coopératives d'économie familiale*), *l'Association des consommateurs pour la qualité dans la construction* (ACQC), as well as individual members.

Union des consommateurs' mission is to represent and defend the rights of consumers, with particular emphasis on the interests of low-income households. Union des consommateurs' activities are based on values cherished by its members: solidarity, equity and social justice, as well as the objective of enhancing consumers' living conditions in economic, social, political and environmental terms.

Union des consommateurs' structure enables it to maintain a broad vision of consumer issues even as it develops in-depth expertise in certain programming sectors, particularly via its research efforts on the emerging issues confronting consumers. Its activities, which are nation-wide in scope, are enriched and legitimated by its field work and the deep roots of its member associations in the community.

Union des consommateurs acts mainly at the national level, by representing the interests of consumers before political, regulatory or legal authorities or in public forums. Its priority issues, in terms of research, action and advocacy, include the following: family budgets and indebtedness, energy, telephone services, radio broadcasting, cable television and the Internet, public health, food and biotechnologies, financial products and services, business practices, and social and fiscal policy.

Finally, regarding the issue of economic globalization, Union des consommateurs works in collaboration with several consumer groups in English Canada and abroad. It is a member of *Consumers International* (CI), a United Nations recognized organization.

Introduction

The development of computing and telecommunications networks has led to the creation of a new concept, known as cloud computing. The cloud in question is actually the symbolic representation of the Internet and is used by engineers when they talk about the Internet[1]. The term "computing" refers to functionalities offered by computers, i.e., calculation or data storage capacities. In other words, cloud computing purportedly offers users the possibility of using the Internet as a place where computer calculation or data storage is made available to the public.

Those solutions appear totally new to some people, but they have a history: certain cloud computing services are currently major players on the Internet. Social networks such as Facebook, online messaging services such as Hotmail, Gmail, Yahoo!Mail, photo storage services such as Flickr, used by a great number of consumers, are in fact cloud computing applications. One of the advantages of these solutions is the possibility of accessing them any time, or almost, thanks to wireless telecommunication networks. Online messaging services are so popular that many consumers only use this type of messaging rather than the one offered to them by their Internet access provider.

This transfer to the "cloud" of computer calculation and data storage capacities, which until recently each user located in his own computer, nevertheless raises certain issues.

The relationship between a consumer and a cloud computing service provider is of course governed by a contract. Such contracts – adhesion contracts – are of course drafted by (or for) companies offering cloud computing services and are intended to protect consumer interests as well as possible. In Canada, certain laws have been adopted to protect consumers. Can those laws apply, in the cloud, to those cloud computing service contracts? If so, do the clauses of those contracts fully comply with Canadian consumer protection provisions?

Cloud computing services notably enable consumers to create documents, save and share drawings, photos, etc., which in some cases are creations under the Copyright Act. In such cases, the works are protected and the copyright holder benefits from certain rights with regard to his works. How do the rights with respect to the use of those works, as provided for in the Copyright Act, apply to the use of cloud computing applications?

Does personal information have the same legal protection in the cloud as on firm ground? Many cloud applications, given that they are free of charge, need their users' personal information to function or even survive. Cloud computing service providers pride themselves on their services being free of charge; still, consumers do pay a price: their personal information, which cloud computing users allow to be collected and used by the company offering them the services. So we must also analyse those services in the light of privacy laws.

While companies as well as consumers use cloud computing, and while types of services are even designed specifically for one or the other of these user categories, our research will focus on consumer issues.

[1] Cloud computing, Wikipedia.org website, [Online] http://fr.wikipedia.org/wiki/Cloud_computing#Historique (page consulted on June 22, 2011).

In the first part of the report, we will define cloud computing. The second part will examine how consumers and companies are adopting such services.

The third part of the report discusses concerns that users may have regarding the way in which cloud computing provides services.

The fourth part presents a legal characterization of cloud computing contracts. Subsequent parts examine the latter in the light of consumer protection laws (part five), the Copyright Act (Part Six) and privacy laws (Part Seven).

The eighth part of our report will focus on possible improvements to contractual practices in the area of cloud computing.

1. Defining Cloud Computing and Ascertaining the Benefits of This Type of Service

While it is essential to define cloud computing, the search for a definition can resemble a real investigation. So what benefits are promised by this emerging concept, so highly touted in the information technology world? This is what we will attempt to clarify. Cloud computing raises fears and criticisms, of course; we will discuss some of them and an overview of solutions that have been put forward or advocated.

1.1 Searching for a Definition of Cloud Computing?

In the course of our research, we have been surprised not to find a unanimously accepted definition of cloud computing. Even a summary search encounters several definitions, which address cloud computing from different angles – from engineers or other information technology experts, from journalists, from North American and European governmental organizations, etc. – and often have an incomplete view. In exploring those definitions, we will try to detect their common features, in order to arrive at a definition of cloud computing that we find relevant and that explains as perfectly as possible what cloud computing truly is.

Unsurprisingly, the definition of cloud computing has been amply discussed on social networks and Internet users' blogs. We think there is no better place than the Web 2.0 – the cloud itself – to begin our search for a definition.

Shane Schick, chief editor of *IT World Canada* magazine, reports discussions he has had with other people in an attempt to define cloud computing on the magazine's blog. He mentions that the ubiquitous talk about cloud computing does not imply a consensus on the definition. From the definitions proposed, he retains that it "*refers (for many) to a variety of services available over the Internet that deliver compute functionality on the service provider's infrastructure (e.g. Google Apps or Amazon EC2 or Salesforce.com). (…)*[2]." This definition resembles that of William Robison, for whom the main feature of cloud computing is "*the ability to run applications and store data on a service provider's computers over the Internet, rather than on a person's desktop computer*[3]."

With that same approach, we also find this definition: "*Le Cloud computing est un ensemble de prestations informatiques, accessibles via Internet, qui peuvent aller du simple stockage de données jusqu'à l'externalisation de pans entiers de l'infrastructure informatique*[4]."

We can already note from those definitions that cloud computing essential refers to services offered through the Internet.

[2] SCHICK Shane, Five ways of defining cloud computing, IT World Canada [Online] http://www.itworldcanada.com/blogs/shane/2008/04/22/five-ways-of-defining-cloud-computing/48746/ (page consulted on May 11, 2011).
[3] ROBISON William J., Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act, 98 The Georgetown Law Journal 1195 (2010).
[4] MARCELLIN Sabine, Cloud computing et risques juridiques [Online] http://www.legalbiznext.com/droit/Cloud-computing-et-risques (page consulted on May 11, 2011)

Shane Schick also observes confusion in attempts to define cloud computing, with each stakeholder (infrastructure provider, service provider, consumer) clarifying his viewpoint, which varies depending on how cloud computing is used.

For example, the following definition, derived from a study funded by Google, presents cloud computing as "*a new way to deploy computing technology to give users the ability to access, work on, share, and store information using the Internet. The cloud itself is a network of data centers – each composed of many thousands of computers working together – that can perform the functions of software on a personal or business computer by providing users access to powerful applications, platforms, and services delivered over the Internet*[5]."

This idea of access to calculation and data storage capabilities is shared by other authors: "*cloud computing provides flexible, location-independent access to computing resources that are quickly and seamlessly allocated or released in response to demand. Services (especially infrastructure) are abstracted and typically virtualised, generally being allocated from a pool shared as fungible resource with other customers. (…)*[6]."

In the United States, the *National Institute of Standards and Technology* (hereinafter "NIST"), an American organization responsible for establishing technological standards, has proposed this draft definition of cloud computing:

> *(…) cloud computing is a model for enabling ubiquitous, 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*[7].

The five essential characteristics taken into account by NIST are:

- *On-demand self-service.* A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.
- *Broad network access*. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g. mobile phones, laptops, and PDAs).
- *Resource pooling.* The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge

[5] Marketspace Point of view, Envisioning the Cloud: The Next Computing Paradigm, RAYPORT Jeffrey F. & Andrew HEYWARD [Online] http://marketspacenext.files.wordpress.com/2011/01/envisioning-the-cloud.pdf (page consulted on May 11, 2011).
[6] BRADSHAW Simon, Christopher MILLARD & Ian WALDEN, Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services, Queen Mary School of Law Legal Studies Research Paper No. 63/2010 [Online] http://ssrn.com/abstract=1662374 (page consulted on May 11, 2011).
[7] National Institute of Standards and Technology, Peter Mell & Timothy Grance, The NIST Definition of Cloud Computing (Draft), Special Publication 800-145 [Online] http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf (page consulted on May 11, 2011).

over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g. country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

- *Rapid elasticity.* Capabilities can be rapidly and elastically released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- *Measured Service.* Cloud systems automatically control and optimize resource use by leveraging a metering capability [fn omitted] at some level of abstraction appropriate to the type of services (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service[8].

We will reprise the three service models below.

NIST's draft definition may be commented on or revised by the public; this tends to confirm our previous observation that a full definition of cloud computing remains to be found. Robison maintains this as well: "*The industry cannot even agree on the meaning of the term "cloud computing*[9]."

Other definitions of cloud computing have been offered by non-profit organizations, notably those with the mission of protecting privacy. For example, in its complaint against Google before the Federal Trade Commission, the *Electronic Privacy Information Center* defines cloud computing as "*an emerging network architecture by which data and applications reside on third party servers, managed by private firms, that provide remote access through web-based devices*[10]."

A report by the *World Privacy Forum* uses a definition similar to that provided by the *Electronic Privacy Information Center*: "*cloud computing involves the sharing or storage by users of their own information on remote servers owned or operated by others and accessed through the Internet or other connections*[11]."

The European Commission has also shown interest in the subject: "*A 'cloud' is an elastic execution environment of resources involving multiple stakeholders and providing a metered service at multiple granularities for a specified level of quality (of service)*[12]."

---

[8] *Ibid.*

[9] ROBISON William J., Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act, 98 The Georgetown Law Journal 1195 (2010).

[10] In the Matter of Google, Inc. and Cloud Computing services, Complaint and Request for Injunction, Request for Investigation and for Other Relief Before the Federal Trade Commission [Online] http://www.google.ca/url?sa=t&source=web&cd=1&ved=0CCIQFjAA&url=http%3A%2F%2Fepic.org%2Fprivacy%2Fcloudcomputing%2Fgoogle%2Fftc031709.pdf&ei=IN7KTer7JYrZgAfLg8zfBQ&usg=AFQjCNFzdWwlvKdQsylcYgBzbuuucUei5Q (page consulted on May 11, 2011).

[11] GELLMAN Robert, Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing, World Privacy Forum, February 23, 2009 [Online] http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf (page consulted on May 11, 2011).

[12] The Future of Cloud Computing, Opportunities for European Cloud Computing Beyond 2010, European Commission [Online] http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf (page consulted on May 11, 2011).

It should also be noted that the Office québécois de la langue française (OQLF), in addition to proposing in its Grand dictionnaire terminologique that the term "cloud computing" be francized into "infonuagique" (while also accepting the terms "informatique intranuage," "informatique nuagière," "nuage informatique," "informatique en nuage," but rejecting "informatique dans le nuage" and "informatique dans les nuages") provides an extremely detailed definition:

> *Modèle informatique qui, par l'entremise de serveurs distants interconnectés par Internet, permet un accès réseau, à la demande, à un bassin partagé de ressources informatiques configurables, externalisées et non localisables, qui sont proposées sous forme de services, évolutifs, adaptables dynamiquement et facturés à l'utilisation.*

The OQLF adds in its notes:

> *L'infonuagique, c'est en fait l'informatique vue comme un service et externalisée par l'intermédiaire d'Internet. Elle fait référence à l'utilisation de la mémoire et des capacités de calcul des ordinateurs et des serveurs répartis dans le monde entier et reliés par Internet. Les ressources informatiques mises en commun et rendues ainsi disponibles à distance peuvent être, entre autres, des logiciels, de l'espace de stockage et des serveurs*[13]*.*

The Privacy Commissioner of Canada also offers a definition, which we think summarizes quite well the meaning of cloud computing:

> *In general, it is the provision of web-based services, located on remote computers, that allow individuals and businesses to use software and hardware managed by third parties. Examples of these 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*[14]*.*

Cloud computing is thus the capability of providing computer services in a new way by means of the cloud. The *National Institute of Standards and Technology* uses classifies according to three models the services deployed through cloud computing[15]: *Software as a Service* (SaaS), *Platform as a Service* (PaaS), *Infrastructure as a Service* (IaaS).

Software as a service (SaaS) is most used by the general public: Facebook, Flickr, Hotmail and others, as well as the various *Google Apps* are found under this banner. Our study will focus on applications of this model.

Software as a service (SaaS) enables users to benefit from online applications by registering or subscribing (free of charge or not) with a provider, rather than purchase a licence for software to

[13] Grand dictionnaire terminologique, definition of cloud computing [Online] http://www.granddictionnaire.com/BTML/FRA/r_Motclef/index800_1.asp (page consulted on May 11, 2011).
[14] Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing [Online] http://www.priv.gc.ca/resource/consultations/report_201105_e.asp (page consulted on May 27, 2011).
[15] Details of these types of services are taken from the document of the National Institute of Standards and Technology, Peter Mell & Timothy Grance, The NIST Definition of Cloud Computing (Draft), Special Publication 800-145 [Online] http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf (page consulted on May 11, 2011).

be installed in their machine. They can thus use their Web browser or another platform to access the application. A consumer using the software service has no way to control the application; he can modify only a few predefined parameters or settings and must use the application as is. In other words, since the software used by means of the cloud is not installed in the user's machine, "*le modèle SaaS permet de déporter une application chez un tiers*[16]*.*"

In data processing, the platform is the support on which one can write, read, use, develop a software package (hardware, operating system and software tools). The platform service (PaaS) enables users to deploy, use and control applications created by using the programming language and the tools offered by the cloud computing service provider directly on a network, servers, operating systems which the user does not control. This model essentially consists of making immediately available to companies a middleware environment with a concealed infrastructure[17]*.* PaaS platforms are notably used as a development and testing environment. The best-known PaaS are *.NET Framework,* the *Microsoft* development platform, and *Force.com.*

The infrastructure service (IaaS) is a model whereby a company has a computer infrastructure (servers, storage, network) that is actually located on the service provider's premises. However, the company has unrestricted access to that infrastructure, as though the hardware were located on its own premises[18]. IaaS provides the user with basic computer resources (calculation, storage, networking and other capabilities) enabling him to deploy and use software, applications and operating systems. The user of this service has no control over its underlying infrastructure, but does control the operating system, storage and applications deployed. The IaaS model provides a hosted computer infrastructure. Thus, a company can, for example, rent Linux, Windows or other types of servers, which actually operate in a virtual machine on the premises of the IaaS provider[19]. IaaS infrastructures of well-known companies are *Amazon Web Services*, *Windows Azure* and *SQL Azure*.

[16] Syntec numérique, Livre Blanc Sécurité du Cloud Computing, Analyse des risques, réponses et bonnes pratiques [Online] http://www.syntec-numerique.fr/actualites/liste-actualites/livre-blanc-cloud-computing-securite (page consulted on May 12, 2011).

[17] http://en.wikipedia.org/wiki/Platform_as_a_service *"*In its most general sense, **middleware** is computer software that provides services to software applications beyond those available from the operating system. Middleware can be described as "software glue". Thus middleware is not obviously part of an operating system, not a database management system, and neither is it part of one software application. Middleware makes it easier for software developers to perform communication and input/output, so they can focus on the specific purpose of their application*."* http://en.wikipedia.org/wiki/Middleware

[18] http://en.wikipedia.org/wiki/Infrastructure_as_a_service#Service_Models

[19] Pro Group. Services we can deliver > Cloud-Computing. [Online] https://sites.google.com/a/pronewtech.eu/pronewtech-en/services/cloud-computing-green-ict (page consulted on January 16, 2012).

1.2 A Few Advantages of Cloud Computing

In its document on the future of cloud computing[20], the European Commission presents some of the latter's advantages. Among these, the Commission mentions "elasticity[21]," i.e., the capability to adapt to the needs of users. For instance, a user who owns a device with limited processing capacity may, for certain uses, temporarily need additional processing capacity (a more powerful processor). Cloud computing offers the user an on-demand processing capacity, which adapts in real time to his specific needs. The consumer is no longer obliged, to perform desired tasks, to acquire a new device with a more powerful processor; cloud computing can give him timely access to those additional resources.

The same applies to companies, whose computer maintenance costs can be reduced thanks to cloud computing services. In fact, cloud computing makes it unnecessary to have a large quantity of computer equipment or servers to accumulate and store data. To those savings are added electricity savings: there is no longer any need to supply the considerable energy required by all such computer equipment. Nor is it necessary to configure those machines or update software and hardware. The latter connects directly to cloud computing services where the latest software versions are already installed on an infrastructure whose maintenance is ensured by the company providing the cloud computing solution.

In addition, users may save by using software offered by cloud computing: the consumer no longer has to purchase licences to use software available by this means. A lot of software is offered online "free of charge" and users can create and modify their documents directly from those applications.

The use of such online software also makes it possible for many people to work on the same document, which is no longer registered on a single user's device, but rather on servers remotely accessible at all times.

At the public consultation and the round table that Canada's Office of the Privacy Commissioner had organized on the subject, some respondents mentioned other advantages[22], such as the reliability of cloud computing services Cloud computing "(*eliminates the concern of losing valuable data in paper format or via the loss of laptops or hard drives*[23]." The efficiency of cloud computing was also emphasized: freeing up resources makes it possible to focus on innovation and product creation. Moreover, cloud computing gives immediate access to the very latest available technologies.

While companies are interested in the three cloud computing service models, consumers mainly use only the first model, i.e., software services. Thus, the present study will mainly discuss this service model.

---

[20] The Future of Cloud Computing, Opportunities for European Cloud Computing Beyond 2010, European Commission p.13 [Online] http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf (page consulted on May 11, 2011).
[21] The term "elasticity" is also used by the National Institute of Standards and Technology, among others. The Privacy Commissioner of Canada uses the term "flexibility."
[22] Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing [Online] http://www.priv.gc.ca/resource/consultations/report_201105_f.cfm (page consulted on May 27, 2011).
[23] *Ibid*.

2 Consumers and Companies Adopting Cloud Computing

Cloud computing includes service offers intended for consumers and other service offers intended for companies. Indeed, consumer and company needs are not entirely identical, nor are the desired benefits. So it can be expected that the level of adoption of cloud computing services is not the same between these two types of users.

2.1 Consumers

a) Adoption by Consumers

A worldwide study of cloud computing conducted in 2010 by KPMG[24], a global network of auditing, tax and consulting services, among 5,627 consumers in 22 countries (including Canada) reveals that 66% of those questioned use cloud computing services. It should be noted that only 19% of consumers questioned as part of that study resided in the Americas. A survey conducted in March 2010 by Harris Interactive among adult American Internet uses indicated that 55% to 69% of respondents were not interested in using cloud computing services[25]. The two studies covered almost identically the same cloud computing services, whether online e-mail or photo services.

A more recent survey conducted on the Internet by *GfK Business & Technology* in 2011 among 1,000 adult Americans reveals that 62% of respondents do not know about cloud computing or do not know what it is[26]. However, that study also indicates that 60% of persons 18 to 35 years of are are interested in the ability to store data in the cloud, and would thus be likely to use such solutions, as opposed to only 25% of persons 50 years of age and over. This result is not very surprising: young people generally adapt new technologies more rapidly than their elders.

b) Services Used by Consumers

A survey conducted in 2008 by *PEW Internet & American Life Project* about the use of cloud computing services and applications by American Internet users[27] reveals that 56% of respondents use online e-mail services such as those provided by *Hotmail*, *Gmail* or *Yahoo! Mail*. In addition, 34% of respondents state that they store personal photos online. Finally, 29%

[24] KPMG, Consumers and Convergence IV- Convergence goes Mainstream: Convenience Edges Out Consumer Concerns over privacy and security, [Online] http://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Pages/Convergence-Goes-Mainstream-O-201007.aspx (page consulted on May 12, 2011).

[25] GONSALVES Antone, Cloud Computing Leaves Consumers Cold, InformationWeek [Online] http://www.informationweek.com/news/hardware/utility_ondemand/224600070 (page consulted on May 12, 2011).

[26] GfK Survey: Cloud Computing Has the Power to Enhance Consumer Data Consumption, But Obstacles Hinder Greater Short-Term Adoption, [Online] http://www.gfkamerica.com/newsroom/press_releases/single_sites/007588/index.en.html (page consulted on May 12, 2011).

[27] PEW/Internet, Use of Cloud Computing applications and services Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing 2008 [Online] http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Cloud.Memo.pdf.pdf (page consulted on May 12, 2011).

of respondents admit to using online applications such as Google Documents or Adobe Photoshop Express. The KPMG study showed that 70% of respondents use online photo storage services and that 68% of respondents use online e-mail services. Finally, 56% of respondents use social network services.

2.2 Companies

a) Adoption by Companies

A *PricewaterhouseCoopers*[28] study conducted in Canada among software company executives reveals that over half (52.4%) of the companies questioned use cloud computing services. 42.7% of respondents consider that cloud computing is extremely important to their business model. But the same study indicates that 32% of those executives consider that cloud computing will have no impact on their operations and therefore do not perceive it as an essential solution for their company.

What cloud computing services are used by the public and companies?

b) Services Used by Companies

A *Markess International*[29] study shows that 12% of private companies and public organizations have already used at least one cloud computing service model. That study also mentions that the most oft-used services were collaborative applications: messaging, shared agendas, Web conferences, etc. However, between 2008 and 2010, companies notably turned toward customer relationship management applications[30] or social applications. A *PricewaterhouseCoopers* study reports that 58.3% of Canadian software company presidents believe that online software services are the most promising. It should be mentioned that the software services proposed to companies and consumers are not entirely the same. Thus, while the software service is also perceived by companies to be most interesting, certain tools, such as customer relation management tools, are resolutely intended for those companies. On the other hand, online e-mail services may meet the needs of consumers and companies alike, even if the software offered to the two clienteles are not the same.

[28] JACOBSON, David H., A view on Cloud Computing, PricewaterhouseCoopers, Toronto, May 2010 [Online] http://www.pwc.com/ca/en/emerging-company/publications/cloud-computing-05-10-en.pdf (page consulted on May 12, 2011).
[29] Markess International, Cloud Computing & SaaS Attentes et Perspectives, Référentiel de pratiques Edition 2010 [Online] http://www.markess.fr/synthese.php (page consulted on May 12, 2011).
[30] "*Customer relationship management (CRM) is a widely implemented model for managing a company's interactions with customers, clients, and sales prospects.*" [Online] http://en.wikipedia.org/wiki/Customer_relationship_management (page consulted on May 27, 2011).

2.3 Motivation of Consumers and Companies

What reasons motivate consumers and companies to adopt cloud computing solutions?

The *PEW/Internet*[31] study notably indicates that 51% of respondents use cloud computing services because it is easier and practical to do so. 41% of respondents invoke accessibility – the ability to access data when and where they want – as a reason to use such services. And 39% of respondents say it is a practical way to share information.

For companies, the main reason for adopting cloud computing services appears, according to the *PricewaterhouseCoopers*[32] study, information technology savings. The study conducted by the *Centre for commercial Law Studies* concurs: "*by sharing resources between a pool of customers and buying infrastructure in bulk, Cloud computing providers can achieve economies of scale that can be passed on to their customers*[33]," which also represents economic incentives for adopting cloud computing services; for example: "*Transforming CAPEX*[34] *to OPEX*[35]*: moving business operations to the Cloud allows a reduction on capital expenditure on in-house IT infrastructure, which is typically front-loaded and subject to depreciation, in favour of more even ongoing operating expenditure*[36]."

While the benefits of cloud computing appear indisputable, it is also important to point out the concerns raised by this new technology, for consumers as well as companies.

[31] PEW/Internet, Use of Cloud Computing applications and services, September 2008 [Online] http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Cloud.Memo.pdf.pdf (page consulted on May 12, 2011).
[32] *Op. Cit.* Note 28.
[33] BRADSHAW Simon, Christopher MILLARD & Ian WALDEN, Contracts for Clouds : Comparison and Analysis of the Terms and Conditions of Cloud Computing Services, Queen Mary School of Law Legal Studies Research Paper No. 63/2010, p. 3 [Online] http://ssrn.com/abstract=1662374 (page consulted on May 11, 2011).
[34] CAPEX is an abbreviation of "capital expenditure". An English-language term designating tangible and intangible investments. CAPEXs include many elements, such as: the initial acquisition cost of the equipment; startup costs; or production adjustment costs. EduBourse [Online] http://www.edubourse.com/lexique/capex.php (page consulted on May 27, 2011).
[35] OPEX means "operational expenditures", i.e., operating expenses, "an ongoing cost for running a product, business, or system." Wikipedia [Online] https://secure.wikimedia.org/wikipedia/en/wiki/Operating_expense (page consulted on May 27, 2011).
[36] *Op. Cit.* Note 33.

3 Concerns Raised by Cloud Computing

The main concern raised by cloud computing is related to security. The *National Institute of Standards and Technology* (NIST) even considers this as an obstacle: "(…) the biggest obstacle facing public cloud computing is security (…)[37]."

The GfK study reveals that 61% of respondents said they were concerned by the security of content stored in the cloud[38]. The *Harris Interactive* survey indicates that 58% of respondents disagree that files stored in the cloud are more secure than those stored locally in a hard disk. It appears that 57% of respondents do not believe it secure to store files in the cloud[39]. 34% of software company executives 34% say that security is the main risk of cloud computing services.

It should be noted that the definition of security used in those studies covers the privacy and protection of personal information. A report by the insurance company *Hiscox* emphasizes some of those risks, particularly those posed by cloud computing to privacy[40]. A privacy violation may have extremely serious consequences for a company, and may push it toward bankruptcy in the event of a lawsuit – for instance, we can imagine the possibility of users' bank data being stolen or made public.

Some studies enable us to refine our analysis of the risks and concerns posed by cloud computing services and to detail the security concerns.

According to the *PEW/Internet* study on the use of cloud computing services and applications[41], 90% of users say they are very concerned that the company storing their data may sell them to a third party. But also, 80% of cloud computing application users say they are very concerned that companies may use their photos and other stored data for advertising purposes. In addition, 68% of those who use at least one cloud computing application say they are very concerned

[37] JANSEN Wayne and Timothy GRANCE, Guidelines on Security and Privacy in Public Cloud Computing, NIST, Draft Special Publication 800-144, [Online] http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf (page consulted on May 12, 2011). By "public cloud" is meant the infrastructure made available to the public or industries by an organization offering cloud computing services. National Institute of Standards and Technology, Peter Mell & Timothy Grance, The NIST Definition of Cloud Computing (Draft), Special Publication 800-145 [Online] http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf (page consulted on May 11, 2011)

[38] GfK Survey: Cloud Computing Has the Power to Enhance Consumer Data Consumption, But Obstacles Hinder Greater Short-Term Adoption, [Online] http://www.gfkamerica.com/newsroom/press_releases/single_sites/007588/index.en.html (page consulted on May 12, 2011).

[39] JACOBSON, David H., A view on Cloud Computing, PricewaterhouseCoopers, *Op. Cit.* Note 28.

[40] Hiscox global technology news, Cloud Computing, Issue 1, Spring [Online] http://www.hiscox.co.uk/_HTML_Emails/Group/technology/cloud_comp/usa/ (page consulted on May 12, 2011).

[41] HORRIGAN John, Use of Cloud Computing Applications and Services, September 12, 2008 [Online] http://www.pewinternet.org/Reports/2008/Use-of-Cloud-Computing-Applications-and-Services/Data-Memo.aspx (page consulted on May 30, 2011).

that the service provider may analyse their personal information and then target advertising to users.

This last result is of great concern because, as we will see below, companies such as Google, Yahoo or Microsoft that provide cloud computing applications actually do targeted advertising. As mentioned above, the *GfK* survey indicated that users do not understand cloud computing services – cloud computing contracts often indicate that targeted advertising will be done (and not only that it may be done) based on the information collected. It clearly appears that users are not aware of or do not understand the provisions of cloud computing contracts.

Apart from these risks, as identified in the studies and surveys mentioned, academics have also been interested in the matter and have put forward certain issues related to cloud computing services – issues of consumer protection, privacy protection and intellectual property.

The study of Dan Svantesson and Roger Clarke, from Bond University, lists a number of concerns or risks related to privacy protection and consumer protection:

> *How data provided to a cloud computing operator will be used by that operator; How such data will be disclosed by the cloud computing operator, and subsequently used by third-parties; The security of the data provided; The legality (under the consumer's local law) of using cloud computing products; Disruptions of the cloud computing service; Getting locked into a contractual arrangement that does not cater for the consumer's future needs, and violating privacy laws by the use of cloud computing products*[42].

On one hand, the authors advise caution to consumers who want to use cloud computing services, and on the other hand hope to have cautioned companies providing those cloud computing services : "*[This article] has also highlighted that consumers using cloud computing products, like other cloud computing users, need to be cautious. The article should also have sent a warning that providers of cloud computing products would do well to familiarise themselves with applicable consumer protection and privacy laws (…)*[43]"

Another major study on cloud computing, that of the *Centre for Commercial Law Studies,* reviewed 31 cloud computing services offered by 27 different providers. The study focused on certain contractual clauses that seemed more problematic, because they contravened consumer protection, intellectual property of privacy laws in effect in Europe. Among the consumer protection clauses analysed, the study examined clauses pertaining to: the law applicable to the contract, the choice of competent jurisdiction or forum, arbitration, unilateral changes to the contract (for example, Secter's contract), the integrity of data stored (for example, Microsoft's contract), guarantees, the liability (or non-liability) of service providers, compensation in case of fault, and service availability[44].

[42] SVANTESSON Dan and Roger CLARKE, "Privacy and Consumer risks on cloud computing," Computer law and security review, 26(4), 391-397 [Online] http://epublications.bond.edu.au/law_pubs/347 (page consulted on May 12, 2011).
[43] *Ibid.*
[44] For examples of clauses, see pages 17 and following of the study by BRADSHAW Simon, Christopher MILLARD & Ian WALDEN, Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services, Queen Mary School of Law Legal Studies Research Paper No. 63/2010 [Online] http://ssrn.com/abstract=1662374 (page consulted on May 11, 2011).

As for privacy protection, this study analysed clauses pertaining to data storage, disclosure and place of conservation and transfer, as well as to service use monitoring.

Regarding intellectual property rights, this study focuses on clauses for content creation and licences granted to application providers in relation to content (for example, Apple iWork's clause).

The study mentions that many if not all cloud computing services are provided by American companies, which tend to use American law in their contracts even when offering services to European consumers. Those contracts thus ignore protection provisions in place in Europe. Under these circumstances, European consumers may turn away from those services and prefer services that meet European protection provisions. The study emphasizes that if American services do not comply with such provisions voluntarily, legislators may intervene to compel companies to do so:

> *Once customers start to note that some providers offer T&C that offer more in the way of enforceable rights than others do, the presence or absence of such rights may well become a selling point. Alternatively, public or administrative law intervention or regulatory pressure may be brought to bear against providers to ensure that, for example, European consumers are offered T&C that are compliant with EU consumer protection law*[45].

Canadian consumers and legislators might also make this choice. Indeed, Canadian consumer protection laws are much more similar to European than American laws.

After comparing the respective advantages of cloud computing for consumers and companies, Cory Doctorow, a well-known science-fiction author, activist, journalist and blogger[46], postulates that cloud computing services meet certain company needs, but that consumers do not necessarily need those services[47]. Cory Doctorow recalls that, to access cloud computing services and transfer their files to the cloud, consumers will need high-speed Internet access, which is not the case for all consumers. Cory Doctorow also points out that the computers currently sold have enormous storage capacities, as well as microprocessors capable of performing almost all tasks performed by consumers' computers, and often much more. One of the primary advantages of cloud computing therefore appears to be very limited for consumers.

[45] BRADSHAW Simon, Christopher MILLARD & Ian WALDEN, Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services, *Op. Cit.* Note 33, p. 46
[46] Cory Doctorow was the European Director of Electronic Frontier Foundation and he co-founded the UK Open Rights Group. [Online] http://craphound.com/bio.php (page consulted on May 13, 2011).
[47] DOCTOROW Cory, Not every cloud has a silver lining, September 2, 2009 [Online] http://www.guardian.co.uk/technology/2009/sep/02/cory-doctorow-cloud-computing (page consulted on May 13, 2011).

4 Legal Characterization of Cloud Computing Contracts

Our study concerns the relation consumers have with cloud computing, rather than the relation companies have with it. This bias will be reflected in the present section, on the legal characterization of cloud computing contracts. It should be remembered that the legal characterization may be different if the user is a company rather than a consumer.

The relation between cloud computing service providers and consumers is of course governed by a contract, which states the parties' respective obligations and services, and which providers call by various names – terms of use, legal notices, general terms or service, service contracts, etc. Companies also publish privacy policies or rules of confidentiality, which detail their commitments to protecting the personal information of cloud computing service users. Those privacy policies or rules of confidentiality also theoretically provide necessary information for a consumer to consent to the companies' collection and use of his personal information.

Some companies call their contracts service agreements; we will examine this below, but it may well not be the only possible characterization.

In the present section, we will try to analyse the contractual relation in order to characterize such contracts adequately. We have chosen to examine this contractual relation according to both civil and common law. To that end, we will refer to Quebec and Ontario laws. Our study will also focus on consumer protection laws; here again, we will examine Quebec and Ontario provincial laws.

4.1 Cloud Computing Contract: Consumer Contracts

To determine whether cloud computing contracts are consumer contracts, our study will review Quebec's applicable laws, i.e., the Civil Code of Québec (CCQ) and the Consumer Protection Act (CPA), and then Ontario's Consumer Protection Act, 2002, S.O. 2002.

a) Quebec

The Civil Code civil of Québec defines the consumer contract as follows:

> (…) *a contract whose field of application is delimited by legislation respecting consumer protection whereby one of the parties, being a natural person, the consumer, acquires, leases, borrows or obtains in any other manner, for personal, family or domestic purposes, property or services from the other party, who offers such property and services as part of an enterprise which he carries on*[48].

We will analyse cloud computing contracts in the light of this first definition of a consumer contract. First, as mentioned above, for the purposes of our study will take as a given that the contracts we attempt to characterize are concluded by consumers, i.e., by natural persons, who use those services for personal purposes.

[48] Civil Code of Québec, section 1384.

The other party to the contract is the one offering cloud computing services. Nicole l'Heureux points out that "*la notion d'entreprise remplace ici celle de commerçant, disparue d'ailleurs partout dans le Code civil (…)*[49]." An *entreprise* is defined as follows in section 1525, subsection 3: "*The carrying on by one or more persons of an organized economic activity, whether or not it is commercial in nature, consisting of producing, administering or alienating property, or providing a service, constitutes the carrying on of an enterprise.*" Given the substantial infrastructures required by cloud computing services, the provision of those services can doubtless be considered an organized economic activity, and thus that of an enterprise, a company.

The consumer contract may concern a good or a service, and the method of acquisition will have no effect on the characterization. A consumer may "acquire, rent, or obtain in any other manner" the good or service – the contract is a consumer contract if the other party makes the offer in the course of his company activities. In theory, a consumer contract could be a gratuitous contract meeting the conditions stated in this section of the Civil Code.

It should be noted that section 1384, C.C.Q., indicates first that a consumer contract is "*a contract whose field of application is delimited by legislation respecting consumer protection (…)*[50]."

The Consumer Protection Act[51] does not redefine the consumer contract, but section 1 defines certain terms to determine, to a certain extent, "the field of application" delimiting the contract to which this Act pertains. The consumer is defined as "*a natural person, except a merchant who obtains goods or services for the purposes of his business*."[52] As with the Civil Code's definition, the consumer may only be, at all times, a natural person[53].

While the consumer is defined in the first section of the Quebec Act, it should be noted that the term "commerçant" is absent from the French version of the Consumer Protection Act. And yet, the English version contains a definition of "merchant" (the English equivalent of "commerçant" in the Act): "*any person doing business or extending credit in the course of his business*[54]." The definition of "merchant" is extremely broad; in this category could easily be included companies providing cloud computing services, so long as their operation constitutes a commercial activity.

[49] L'HEUREUX Nicole, Droit de la consommation, 5th edition, Les Éditions Yvon Blais, Cowansville, 2000, p. 37
[50] Ibid.
[51] R.S.Q., chapter P-40.1.
[52] Consumer Protection Act, R.S.Q., chapter P-40.1, section 1.
[53] On this point, see L'HEUREUX Nicole, Droit de la consommation, 5th edition, Les Éditions Yvon Blais, Cowansville, 2000, p. 36: "Le *Code civil du Québec*, par la définition de l'article 1384, traduit l'intention de protéger le consommateur, 'personne physique.' La CPA protège également le consommateur personne physique, ce qui exclut les sociétés commerciales et les sociétés civiles." Benoît MOORE adds, on the similarities between the definitions of "consumer" in the CPA (Consumer Protection Act) and the Civil Code of Québec: "*Ainsi, tout comme dans la Loi sur la protection du consommateur, le consommateur se limite, dans le Code civil, à la personne physique et doit agir à des fins personnelles, familiales ou domestiques*." MOORE Benoît, Sur l'avenir incertain du contrat de consommation, 49 Les Cahiers de droit (2008) p.5.
[54] Consumer Protection Act, R.S.Q., chapter P-40.1.

Legal doctrine has developed a more complete definition of "merchant" ("commerçant"):

> *En droit, privé, il [le commerçant] était défini comme celui qui exerce des opérations commerciales à l'état professionnel. La qualité de commerçant nécessite la présence de deux éléments. Le premier consiste dans l'exercice d'une activité dans un but de profit. Le second dans le caractère de permanence de l'activité sans qu'il doive s'agir nécessairement de l'activité principale ni même unique de l'opérateur. L'activité doit cependant s'exercer de façon habituelle plutôt qu'occasionnelle*[55].

The second element of this definition poses no problem in the case of interest to us here: companies providing cloud computing services do so continuously and habitually.

Under the Consumer Protection Act, the requirement of exercising the activity to obtain a profit has to be mitigated, since section 3 states that "Non-profit legal persons cannot invoke their non-profit status to avoid the application of this Act." That being said, we will see below that companies offering consumers cloud computing services free of charge are not charitable organizations, but do actually operate for speculative purposes.

This speculative nature remains central to the characterization of the merchant. Caselaw and legal doctrine generally refer, in defining the merchant, to the theory of merchantability: a merchant is one who acts for speculative purposes, habitually and on his own behalf[56].

b) Ontario

The consumer agreement is defined as follows in the Consumer Protection Act, S.O. 2002: "*an agreement between a supplier and a consumer in which the supplier agrees to supply goods or services for payment*[57]*."*

The Consumer Protection Act, S.O. 2002 of Ontario defines the consumer similarly to the Civil Code of Québec definition, which insists on the purpose of the transaction, but unlike the Civil Code it does not define the transactions in question. The 2002 Act states that the consumer is "*an individual acting for personal, family or household purposes and does not include a person who is acting for business purposes*[58]*."*

To designate the party that concludes a consumer contract with the consumer, the Act uses the term *supplier* rather than *merchant*, the supplier being "*a person who is in the business of selling, leasing or trading in goods or services or is otherwise in the business of supplying goods or services, and includes an agent of the supplier and a person who holds themself out to be a supplier or an agent of the supplier*[59]*.*" This definition leaves no doubt that companies providing cloud computing services can be characterized as suppliers under the Act; it should be noted that the Act, to ensure that all types of goods or services are included, specifies "*or is otherwise in the business of supplying goods or services.*"

While the definition of consumer agreements resembles the one found in Quebec law, it should be noted that the Ontario law leaves no doubt as to the necessity, for there to be a consumer

[55] L'HEUREUX Nicole, Droit de la consommation, 5th edition, Les éditions Yvon Blais, Cowansville, Quebec, 2000, p. 30.
[56] Pacific National Leasing Corporation v. Rose, [2001] R.J.Q. 78 (C.A.).
[57] Consumer Protection Act, S.O. 2002, chapter 30, section 1.
[58] *Ibid.*
[59] *Ibid.*

agreement, of payment by the consumer in exchange for the supply of the good or service ("*for payment")*.

However, it cannot be concluded that there cannot be a consumer agreement without payment of an amount of money, since the payment may be "*consideration of any kind, including an initiation fee*[60]*."*

c) "Gratuitous Contracts" and "Consumer Contracts"

Does the requirement, for a transaction in which a consumer participates to be considered a consumer contract, that there be an activity for profit under Quebec law and for payment under Ontario law mean that "gratuitous contracts" are disqualified from being consumer contracts?

The question is asked today with all the more acuity because in Quebec, a Superior Court judge[61] has declared that a cloud computing service agreement was not a consumer agreement since it was concluded gratuitously. Our verifications indicate that the decision was not appealed.

The facts at the origin of this case may be summarized as follows: a *Facebook* user applied to the Court for leave to launch a class action against the company, which had, without adequately informing users beforehand, modified its terms of use of the service in order to allow the social network's users' personal information to be more broadly disseminated.

Judge Déziel, who readily admitted that the contract concluded by *Facebook* users was an adhesion contract[62], concluded that it cannot be a consumer contract, since access to *Facebook* is entirely free of charge and that, in his view, only an onerous contract may be characterized as a consumer contract:

> *[51] Although there exists an adhesion contract, Facebook does not have a consumer relationship with its Users.*
>
> *[52] Access to the Facebook website is completely free.*
>
> *[53] Therefore, there exists no consumer contract when joining and accessing the website, because it's always free.*
>
> *[54] A consumer contract is premised on payment and consideration. It must be an onerous contract as written by the Author Nicole L'Heureux.*
>
> *"Le mot "service" n'est pas défini dans la CPA, on doit lui donner son sens courant d'exercice d'une activité, d'un travail, acheté ou loué pour le bénéfice d'une personne, ou d'une prestation fournie en relation avec la vente ou la réparation d'un bien. Le service se classe dans la catégorie des biens meubles incorporels. On le définit en effet comme "toute prestation qui peut être fournie à titre onéreux, mais qui n'est pas un bien corporel. (…)"*
>
> *[55] Users pay Facebook nothing at all. In joining and accessing the website, Users:*
>
> *"(a) do not pay Facebook;*
>
> *(b) do not undertake to pay Facebook at a later date;*
>
> *(c) do not undertake to remain Users for any period of time;*
>
> *(d) do not undertake to post anything on the Website;*
>
> *(e) do not undertake to encourage friends or family to join the Website; and*
>
> *(f) do not undertake to promote the Website in any way."*

[60] *Ibid.*

[61] In the case of St-Arnaud v. Facebook Inc. 2011 QCCS 1506.

[62] Section 1379 of the Civil Code of Québec provides that: "*A contract of adhesion is a contract in which the essential stipulations were imposed or drawn up by one of the parties, on his behalf or upon his instructions, and were not negotiable.*(…)"

It is understood that this question of characterizing or not a cloud computing contract as a consumer contract appears crucial to us. All cloud computing contracts that have been selected in our study are adhesion contracts, but many of the most popular cloud computing services (all online e-mail services, services such as *Facebook*, *Flickr* and *Picasa*, certain online storage services) are proposed to consumers free of charge – would all consumers using those services deprived of the benefits of consumer protection laws?

With respect, we may question Judge Déziel's conclusions, on the basis of a simple question: is a service offered free of charge necessarily offered at no cost?

There will obviously be no monetary payment obligation for a service offered free of charge. But it should be point out that payment is not necessarily monetary. Under section 1553 of the Civil Code of Québec, "*Payment means not only the turning over of a sum of money in satisfaction of an obligation, but also the actual performance of whatever forms the object of the obligation."* The Ontario Act of 2002 specifies, as we have seen, that payment means "*consideration of any kind."*

Judge Déziel rightly mentions that the user does not have to pay *Facebook* any money – not when the contract is concluded, not when the service is used, and not at any other time. The judge also states that the user has no obligation to recruit members, or even to actively use the account provided to him by the company.

However, the absence of certain obligations does not mean the absence of any obligation.

We stated above without hesitation that cloud computing companies qualify as commercial enterprises. While they provide consumers with certain services free of charge, their commerce is elsewhere: their sources of profits, their speculative goals do not depend on users making monetary payments – which these companies often do not require – but on the commerce of personal information.

Facebook's economic model, like that of many cloud computing companies, rests on advertising and the fact that users will provide such companies with personal information they can sell advertisers, while offering the latter the possibility of displaying their advertisements to a target public. To be persuaded of this, we have only to read what Nick O'Neill reported on *Facebook*'s ability to do targeted advertising:

> *Over the past few years Facebook has increased their targeting capabilities, including the ability to limit advertising to metropolitan areas as well as the following target variables: gender, age, network (workplace, school, etc.), profile keywords, relationship status, and more. Facebook recently released the Facebook Ads API which provides large ad buyers with the ability to build robust ad managers on top of the Facebook advertising platform*[63].

In an article published on the website *Internet Business Insider*, Nicholas Carlson reveals the amount and source of *Facebook*'s revenues in 2009:

> *Self-service ads, which appear on the right side of the screen on Facebook, accounted for about $250 million to $300 million. (…) Engagement ads, which seek user-interaction (and sometimes feature user-endorsements), brought in $100 million. As a part of a 2007 ad deal, Microsoft sells*

[63] O'NEILL Nick, The Secret to How Facebook Makes Money, [Online] http://www.allfacebook.com/facebook-makes-money-2010-01 (page consulted on May 16, 2011).

> *some ads on Facebook. It's payment for the privilege reached $50 million in 2009. Finally, Facebook Gifts and other virtual goods account for between $30 million and $50 million in 2009*[64].

The economy of this business model is perfectly summarized by:

> *By sharing their data with the cloud provider, users make possible the advertising services that pay for the costs associated with providing the cloud service —a model familiar to radio listeners and television viewers who have long accepted commercials embedded in programming to offset some or all of its cost*[65].

While the analogy with radio and television is vivid (a service offered free of charge by a company making money from advertising), it is misleading: radio and television sell advertising on an estimated number of listeners or viewers – the users do not provide any consideration. This is the difference with cloud computing services.

We mentioned above the obligations that users do not have to meet toward *Facebook*. A careful examination of the terms of service actually reveals a consideration that the user must provide – a consideration that, unsurprisingly, is directly linked to the lucrative practices of targeted advertising.

In fact, users pledge to provide *Facebook*, in consideration of the provision of the cloud computing service, with certain personal information, pledge that this information is accurate, and pledge to keep it up to date[66].

[64] CARLSON Nicholas, How Does Facebook Make Money?, Business Insider, May 18, 2010, [Online] http://www.businessinsider.com/how-does-facebook-make-money-2010-5 (page consulted on May 16, 2011).
[65] ROBISON William J., Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act, 98 The Georgetown Law Journal 1195 (2010) 1214.
[66] Statement of Rights and Responsibilities, section 4 (October 4, 2010 version) [Online] https://www.facebook.com/terms.php?ref=pf (page consulted on May 16, 2011). The section continues with a long list of obligations and prohibitions that the Facebook user pledges to observe. Section 10 mentions that "*Our goal is to deliver ads that are not only valuable to advertisers, but also valuable to you*."

William J. Robison summarizes well this price paid by users of such "free" services:

> *In essence, a customer's privacy is the true cost of "free" cloud computing services*[67].

A large part of the interest in or popularity of *Facebook* derives from the website offering the possibility of using applications, games, questionnaires, etc. But here again, one should be perfectly aware that when *a Facebook* user decides to use an application, what the user has provided as content – whether comments, links to websites, and even personal information – will be accessible to the creators of the application in question[68].

It therefore appears difficult to claim that, given the "payment" pledged by users, a service such as that of *Facebook* is "free" and that, at least in Quebec, it could escape the Consumer Protection Act. The future will tell whether caselaw will confirm this recent legal ruling and whether the other Canadian provinces will follow suit.

4.2 Service Contracts, Contracts Involving Sequential Performance, Contracts Involving Sequential Performance for a service provided at a distance, and Internet Agreements

We have already mentioned the variety of designations that companies may give cloud computing contracts. At first sight, it would appear obvious to call them service agreements. But should we stop at that assumption?

a) Quebec

Section 2098 of the Civil Code of Québec defines a service agreement ("*contract for services*") as *"(…) a contract by which a person, the contractor or the provider of services, as the case may be, undertakes to carry out physical or intellectual work for another person, the client or to provide a service, for a price which the client binds himself to pay*[69]*."* (Our emphasis)

The issue raised by this section concerns the price that the customer pledges to pay – this payment of a "price" being a determinant of the very definition of service agreements. Should we conclude that a gratuitous contract cannot be a service contract, even if it meets all the other conditions?

Regarding cloud computing services said to be payable, i.e., those whose subscription or use is charged monetary fees, the application of this definition seems to leave no doubt: the service provider pledges to provide the user with the service for the price displayed or proposed, which the user pledges to pay.

But in the case of cloud computing services offered free of charge, can we consider that the user will still pay "a price?" As we argued in a previous section ("Gratuitous" Contracts and Consumer Contracts), we think it reasonable to consider as a price paid by the customer the mandatory disclosure of personal information that will be used by companies providing cloud computing services for profit.

[67] *Op. Cit.* Note 65.
[68] *Op. Cit.* Note 66.
[69] Civil Code of Québec, section 2098.

These cloud computing contracts are certainly contracts of successive performance in the sense of the second paragraph of C.C.Q. section 1383: "*Where the circumstances absolutely require that the obligations be performed at several different times or without interruption, the contract is a contract of successive performance*[70]." As pointed out by Vincent Karim, it is a contract whereby "*les obligations s'exécutent en plusieurs fois, à court ou à long terme*[71]." In fact, there is a "*contrat à exécution successive lorsque l'exécution instantanée est impossible*[72]," as may be the case with, for instance, a sales contract, whereby the parties' respective obligations, the payment and the property transfer may be completed almost simultaneously.

Cloud computing services are dematerialized and the service is provided through communications networks, and thus remotely. This type of contract may therefore be characterized as a *contract of successive performance for a service provided at a distance*. This type of contract, which is named and regulated in the Consumer Protection Act (in sections 214.1 and following), is not given any particular condition there, so the correspondence of the service with the essential terms used for defining this type of contract makes it easy to apply this characterization to cloud computing.

Cloud computing contracts are as a rule (to which we know of no exception) contracts for a service provided at a distance, through the Internet, by means of communications networks. Section 54.1 of the Consumer Protection Act defines this type contract as follows: "*a contract entered into without the merchant and the consumer being in one another's presence and preceded by an offer by the merchant to enter into such a contract*[73]."

However, it should be noted that these two characterizations will apply only to contracts to which the Consumer Protection Act itself applies.

b) Ontario

Somewhat similarly, cloud computing contracts may in Ontario be legally characterized as distance contracts (the equivalent of distance contracts referred to in Quebec's Consumer Protection Act), Internet contracts and contracts of successive performance.

Section 20 of the Consumer Protection Act, S.O. 2002 defines the distance contract (*remote agreement*) as follows: "*a consumer agreement entered into when the consumer and supplier are not present together*." As we have seen, this is the case with the conclusion of a cloud computing contract.

The rules governing an Internet contract also apply to a cloud computing contract, since in both cases there is "*a consumer agreement formed by text-based internet communications*[74]*."*

The Ontario law defines what a contract of successive performance (*future performance agreement*) is: "*a consumer agreement in respect of which delivery, performance or payment in full is not made when the parties enter the agreement*[75]." We may also retain this characterization for cloud computing contracts, since the company's service provision does not

[70] *Ibid.*, section 1383.
[71] KARIM Vincent, Les obligations, Volume 1, Wilson & Lafleur Ltée, 2009, p. 197.
[72] *Ibid*, p. 200.
[73] Consumer Protection Act, R.S.Q., chapter P-40.1, section 54.1.
[74] Consumer Protection Act, S.O. 2002, section 20.
[75] *Ibid,* section 1.

take place at the moment when the contract was entered into, but will take place over time. We may consider this characterization to be similar to that in Quebec regarding contracts of successive performance.

4.3 Conclusion

In short, a cloud computing contract may be characterized as follows:

- Adhesion contract, in Quebec, because the terms are imposed on the consumer, who cannot negotiate them;
- Consumer contract, in Quebec, or consumer agreement, in Ontario, given the persons who are parties to the cloud computing contract are consumers and merchants (suppliers, in Ontario)[76];
- Service contract, in Quebec, so long as one may consider the user's provision of personal information as the price of the service;
- Contract of successive performance, in Quebec, because the provision of cloud computing services is not instantaneous, but takes place over time;
- Future performance agreement, in Ontario, because the provision of cloud computing services is not instantaneous, but takes place over time;
- Distance contract, in Quebec, because the parties are not in the presence of one another when the merchant offers the consumer to enter into such a contract;
- Remote agreement, in Ontario, because the consumer and the supplier are not in the presence of one another at the moment when the contract is entered into;
- Contract of successive performance involving a service provided at a distance, in Quebec, both because the cloud computing services are not executed instantaneously and because the service is provided at a distance, i.e., the company provides the service without being in the consumer's presence;
- Internet agreement, in Ontario, because the cloud computing contracts are formed by text-based internet communications.

The legal characterization of cloud computing contracts being established, we can on this basis examine cloud computing contract clauses in order to determine whether the rules governing these types of contract are well applied.

In the following sections, we will choose certain contracts and examine some of their clauses, particularly on the basis of the issues raised in the literature.

[76] However, a recent decision by the Superior Court of Québec has rejected as baseless such a qualification regarding contracts.

5. The Choice of Applications to Be Examined

On the basis notably of the studies mentioned above[77], we have observed that certain types of cloud computing applications are more popular than others. The public has mainly adopted solutions known as "Software as a Service;" two types of applications stand out – those for sending and receiving e-mail, and those for storing photos or other files online. We have of course chosen to focus on these types of applications. But it should be noted that another type of application is immensely successful on the Internet: social networks, led by Facebook. Accordingly we have also selected this application for analysis.

We have selected the three e-mail applications currently most used in Canada: *Hotmail* from *Microsoft, Yahoo! Mail* from *Yahoo!* and *Gmail* from *Google*[78].

One of the major players in online data storage applications is the *Rackspace* corporation; given that its services are mainly intended for companies, we have not selected *Rackspace*'s services. We have instead chosen *Flikr*, an online photo storage and sharing service offered by *Yahoo!*. *Google* offers *Picasa*, a somewhat similar service, which we will also study.

The cloud offers many data storage and sharing solutions. Services such as *Adrive*, *Dropbox*, *Zecter Zumodrive*, and *MobileMe* are currently services of this type that are most used by consumers. Certain contractual provisions of many of these services have been analysed by the *Centre for Commercial Law Studies*, from a European and British viewpoint. We will study contractual provisions from the viewpoint of Canadian law. We will also examine the contact of *Norton Online Backup*, an online storage service billed on an annual basis.

In terms of social networks, Facebook is considered the major player, so choosing to study the contractual provisions of this service seemed inevitable to us.

Finally, the other cloud computing applications we have selected are word processing services and other office tools. The applications we have selected are offered by large companies that, here again, dominate the sector. We have chosen *Google docs*, *Zoho Services* and *Office Web Apps,* a service ancillary to *Microsoft*'s *Hotmail* service.

We previously discussed certain risks related to cloud computing services. Those risks primarily involve consumer protection, privacy protection and copyright. In the following sections, we will analyse in detail the clauses of cloud computing contracts selected, in order to determine

[77] PEW/Internet, Use of Cloud Computing applications and services, September 2008 [Online] http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Cloud.Memo.pdf.pdf (page consulted on May 12, 2011); KPMG, Consumers and Convergence IV- Convergence goes Mainstream: Convenience Edges Out Consumer Concerns over privacy and security, [Online] http://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Pages/Convergence-Goes-Mainstream-O-201007.aspx (page consulted on May 12, 2011).

[78] BROWNLOW Mark, Email and webmail statistics, [Online] http://www.email-marketing-reports.com/metrics/email-statistics.htm (page consulted on May 13, 2011); According to this section, there is no specific study on the use of e-mail services; but based on public data, Mark Brownlow determined that the four main online e-mail services are Hotmail, Yahoo!Mail, Gmail, and AOL Mail. The latter service is popular mainly in the United States; hence we did not choose it.

whether some of those contracts pose risks, or whether they might not comply with the laws mentioned.

5.1 Analysis of Cloud Computing Provisions in the light of Consumer Protection Laws

In the contracts we examined, we saw various clauses that seemed problematic with regard to consumer protection laws and the Civil Code: waiver of liability clauses, warranty exclusion clauses, clauses submitting the contract to foreign laws or jurisdiction, unilateral alteration and termination clauses. We will then discuss consumer remedies and the sanctions that companies may face.

We will systematically examine the contracts of all the services we have selected: those of *Apple*'s *MobileMe*; *Facebook*; *Adrive*; *Dropbox*; *Google docs, Gmail and Picasa* from *Google*; *Hotmail* and *Office Web Apps* from *Microsoft*; *Yahoo!Mail* and *Flickr* from *Yahoo!; Zoho* and *Zumodrive*, as well as *Norton Online Backup*. In each section, we will systematically mention all the clauses examined. When the contract for a cloud computing service is not mentioned in a given section, it is because the contract for that service does not contain the type of clause analysed.

Some of those services are offered for monetary payment (*Norton Online Backup*, for example, requires an annual subscription), others are offered free of charge for the basic service and at a monetary price for additional services (for example, to obtain additional storage capacity at *Dropbox*, *Adrive*, etc., or to use certain advanced features for collaborative work at *Zoho*). However, as we have mentioned, many of those cloud computing services are provided without consumers having to pay any amount of money. Despite the Superior Court decision in the *Facebook* case, we will consider all cloud computing contracts as consumer contracts and will apply the provisions of the Consumer Protection Act to the analysis of those various contracts.

The cloud computing companies selected offer their services indiscriminately to consumers of all Canadian provinces; the contracts offered are identical, whatever the user's province of origin.

Some of the clauses examined are identical from one company to another; to lighten the text, we will only quote some examples of those clauses. All the clauses studied will be fully reproduced in annex.

a) Language of the Contract

We have observed that most cloud computing contracts are written in English and that often no French version is available – with the exception of certain large companies, such as Microsoft, Apple and Google, which produce French-language contracts. However, section 26 of the Consumer Protection Act states that "*The contract and the documents attached thereto must be drawn up in French. They may be drawn up in another language if the parties expressly agree thereto. (…)*[79]."

[79] CPA section 26 applies to contracts of successive performance for a service provided at a distance, as specified in section 23: "This chapter applies to contracts which, under section 58, 80, the first paragraph of section 150.4, section 158, 190, 199, 208 or 214.2, must be evidenced in writing."

The infraction appears evident: we wonder when and how Quebec consumers who use cloud computing services would have explicitly expressed their desire that all those contracts be written and available in English only.

b) Waiver of Responsiblity Clauses

In Quebec consumer law, a merchant cannot waive, by a contract stipulation, his liability for what results from his personal action or that of his representative[80]. Rather than simply providing that this type of stipulation would be invalid, section 10 of the Consumer Protection Act goes so far as to prohibit this type of stipulation: "*Any stipulation whereby a merchant is liberated from the consequences of his own act or the act of his representative is prohibited* [81]." It should be specified that, because many companies offer their services over the entire Canadian territory, and because requiring distinct adhesion contracts for Quebec consumers – contracts where the prohibited clauses would not appear – could be an excessive burden on companies usually using the same contract whatever their customers' place of residence, the Quebec legislature has mitigated the Act. If a contract offered to a Quebec consumer contains a clause prohibited by the Act, the contract must clearly indicate, under section 19.1 of the Act, that the clause in question is inapplicable in Quebec: "19.1. *A stipulation that is inapplicable in Québec under a provision of this Act or of a regulation that prohibits the stipulation must be immediately preceded by an explicit and prominently presented statement to that effect*."

Sections 1472, 1474 and 1476 of the Civil Code of Québec recognize "*la validité de ces clauses exonératoires, sauf lorsqu'elles s'appliquent au préjudice corporel ou moral (…). En outre, dans tous les cas, il impose comme condition qu'elles ne puissent pas servir à exclure ou limiter le dommage résultant de la faute lourde ou intentionnelle*[82]." However, the abusive nature of such a clause could be raised by consumers, as Beaudoin emphasizes: "*Rappelons que, dans un contrat d'adhésion ou de consommation, il ne faut jamais oublier la possibilité de faire annuler ou réduire une stipulation quelconque, y compris une clause exonératoire* (…)[83]." The author adds: "(…) *selon une tendance récente, la clause exonératoire devrait être paralysée lorsqu'elle touche la principale obligation, le cœur même du contrat*[84]."

In Ontario, the Consumer Protection Act, S.O. 2002 does not contain a provision similar to section 10 CPA; a common law principle, the doctrine of "fundamental breach," nevertheless recognizes certain limits to the exclusion of liability:

> *an exculpatory clause will not be applied or interpreted in such fashion as to render nugatory or illusory the obligations of one party. Further, Canadian courts continue to interpret clauses strictly on the basis of the* contra proferentum *principle. (…) It may be observed that the Canadian common law doctrine, which appears to confer a residual discretion on courts to refrain from applying exculpatory clauses in cases where this lead to unconscionable, unfair and unreasonable results, appears to have some similarity to the English statutory scheme that enables courts to withhold enforcement*

[80] L'HEUREUX Nicole, Droit de la consommation, 5th edition, Les éditions Yvon Blais, 2000, p. 54.
[81] Consumer Protection Act, R.S.Q., chapter P-40.1, section 10.
[82] BAUDOUIN, Jean-Louis and Pierre-Gabriel JOBIN, Les Obligations, 5th edition, Éditions Yvon Blais, Cowansville, 2005, p. 950.
[83] *Ibid.*
[84] *Ibid*.. p. 952

> *of such clauses* "*except in so far as… the contract term satisfies the requirement of reasonableness (…)*[85]."

We conclude that, while such a waiver of liability clause is prohibited in Quebec, it could legally be found in contracts applicable in common law provinces. However, should a waiver of liability clause "*lead to unconscionable, unfair and unreasonable results*" or "*render nugatory or illusory the obligations of one party,*" the court may, under certain conditions, conclude that there are inapplicable. Ideally, if this type of clause is prohibited or inapplicable, it should not be found in consumer contracts, because it leads consumers to believe, when told that the contract constitutes the law between the parties, that it will be applicable.

And yet, many cloud computing contracts contain waiver of liability clauses. We have found this type of clause in the online storage contracts of *Zumodrive*, *Dropbox*, *Norton Online Backup* and MobileMe[86]. We have also found this type of clause in the contract of Zoho, an online office software service.

An example of this type of clause is section 10 of Zumodrive's Terms of Service, which clearly (and exhaustively) states that the company cannot be held liable:

> *You expressly understand and agree that Company shall not be liable for any direct, indirect, incidental, special, consequential or exemplary damages, including but not limited to, damages for loss of profits, goodwill, use, data or other intangible losses (even if Company has been advised of the possibility of such damages), resulting from: (i) the use or the inability to use the Service; (ii) the cost of procurement of substitute goods and services resulting from any goods, data, information or services purchased or obtained or messages received or transactions entered into through or from the Service; (iii) unauthorized access to or alteration of your transmissions or data; (iv) statements or conduct of any third party on the Service; (v) or any other matter relating to the Service*[87].

As we mentioned, a contract proposed to Quebec consumers, should it contain a prohibited clause, must mention before the clause in question, in an evident and explicit manner, that the clause is inapplicable in Quebec (19.1 CPA).

Some of the contracts examined mention the *possible* non-application of *certain* jurisdictions. This type of mention is found in the terms of service of: *Yahoo!*, for all services provided by the company (and thus for *Flickr* and *Yahoo!Mail) (*section 20[88]*)*; *Apple*'s *MobileMe* (section 13[89]); Microsoft, for all its services (section 10[90]); *Adrive* (section 16[91]); *Google,* for all its services

[85] McCAMUS John D., The Law of Contracts, Irwin Law, 2005 pp. 776-777.
[86] The contracts' relevant provisions are reproduced in annex.
[87] Zumodrive Terms of Service, section 10 [Online] http://www.zumodrive.com/tos (page consulted on May 17, 2011).
[88] Yahoo! Canada Terms of Service, [Online] http://info.yahoo.com/legal/ca/yahoo/utos/utos-ca01.html (page consulted on May 17, 2011). Section 1: "In addition, when using particular Yahoo! services, you may be subject to guidelines or rules or additional terms (which may be posted from time to time) applicable to such services and which are incorporated by reference into the TOS. All such guidelines or rules are hereby incorporated by reference into the TOS."
[89] MobileMe, Terms of Service [Online] http://www.apple.com/legal/mobileme/en/terms.html (page consulted on May 17, 2011).
[90] Microsoft, Service Contract, section 10 *in fine*: "Some or all of these limitations or exclusions may not apply to you if your state, province, or country does not allow the exclusion or limitation of incidental,

(section 14.1[92]); *Facebook* (section 15.3[93]); and *Symantec*'s *Norton Online Backup* (section 11[94]).

For example, *Yahoo!*'s contract contains, following the waiver of liability clause (sec. 19), the following mention:

> *Some jurisdictions do not allow the exclusion of certain warranties, representations and conditions or the limitation or exclusion of liability for incidental or consequential damages. Accordingly, some of the above limitations of sections 18 and 19 may not apply to you.*

A competitor, *Apple*, uses similar wording in the contract for its *MobileMe* service, prior to the waiver of liability clause:

> *Some jurisdictions do not allow the exclusion of certain warranties, as such, to the extent such exclusions are specifically prohibited by applicable law, some of the exclusions set forth below may not apply to you.*

We thus observe that some companies are aware of the peculiarities of certain laws prohibiting waiver of liability clauses. However, the simple fact of mentioning that certain jurisdictions do not allow a waiver of liability clause does not suffice to meet the CPA's requirements. Indeed, in Quebec, given that the waiver of liability clause is inapplicable because prohibited, a mention should, under CPA section 19.1, precede this inapplicable clause, not follow it. The waiver of liability clause should also be more explicit: a simple mention that certain jurisdictions may, to a certain extent, restrict the application of a waiver of liability clause cannot suffice. The clause in question should, under the CPA, indicate that this clause does not (rather than "may not") apply in Quebec (rather than "some jurisdictions"). We must conclude that the companies do not comply with Quebec's Consumer Protection Act.

The smaller companies providing cloud computing services appear to completely ignore not only the laws prohibiting waiver of liability clauses, but also the obligation, should such a clause be included, to mention its inapplicability in Quebec.

consequential, or other damages." [Online] http://windows.microsoft.com/en-145/windows-live/microsoft-service-agreement (page consulted on June 26, 2011).

[91] Adrive, Terms of Service [Online] http://www.adrive.com/terms (page consulted on May 17, 2011).

[92] Google, Terms of Use [Online] http://www.google.com/accounts/TOS (page consulted on May 17, 2011).

[93] Facebook, Statement of Rights and Responsibilities [Online] http://www.facebook.com/terms.php?ref=pf (page consulted on May 17, 2011).

[94] Norton Online Backup. Terms of service agreement. [Online] http://www.symantec.com/content/en/us/about/media/NOBU_TOS_21_USE.pdf (page consulted on January 16, 2012).

c) Warranty Exclusion Clauses

The object of cloud computing contracts is not to deliver a thing or a good, but rather services. But warranties can also apply to services.

The Civil Code contains provisions regarding service contract warranties. Sections 2100[95] and 2102[96] notably impose on the service provider a general obligation of caution and diligence – the obligation to act in the customer's best interests – but also that of disclosing the nature of the task to be performed. The warranty also applies, of course, to the compliance of the service provided with that provided in the contract[97].

In the Consumer Protection Act, section 34 of the "Warranties"[98] Division determines the scope by specifying that warranties apply both to service contracts and to goods[99]. Accordingly, under section 40 of the Act, "*The goods or services provided must conform to the description made of them in the contract*[100]*.*"

Regarding legal warranties applying to services, Nicole L'Heureux mentions:

> *Ce dernier [le consommateur], en concluant un contrat pour la fourniture d'un service, a le droit de recevoir un service qui soit conforme et sûr, tout comme lorsqu'il se procure un autre bien. Une agence de voyages qui fournit des prestations déficientes doit assumer la garantie de ses services de la même façon qu'un garagiste doit le faire. La notion d'attente légitime pourrait permettre au tribunal d'apprécier l'étendue des obligations du prestataire de services*[101].

In addition to what is provided in the contract and announced by the service provider in any declaration or advertisement, the service provider would thus be obliged to offer the consumer a warranty that corresponds to his legitimate expectations.

What are the legitimate expectations of consumers with regard to cloud computing contracts? The user who uses a data storage service should reasonably expect that the company storing the data does not lose or delete them and that it enables access to them at all times. As for online e-mail services, consumers may of course legitimately expect to be able to access the service at all times; to receive messages as quickly as possible; and, as with data storage services, to be able to keep their e-mail, since storage capacity is offered to them for that purpose.

---

[95] Civil Code of Québec, section 2100: "The contractor and the provider of services are bound to act in the best interests of their client, with prudence and diligence. Depending on the nature of the work to be carried out or the service to be provided, they are also bound to act in accordance with usual practice and the rules of art, and, where applicable, to ensure that the work done or service provided is in conformity with the contract.(…)"

[96] Civil Code of Québec, section 2102: "Before the contract is entered into, the contractor or the provider of services is bound to provide the client, as far as circumstances permit, with any useful information concerning the nature of the task which he undertakes to perform and the property and time required for that task."

[97] L'HEUREUX Nicole, Droit de la consommation, 5th edition, Les éditions Yvon Blais, 2000, p. 65.

[98] Consumer Protection Act, R.S.Q., chapter P-40.1, Title I, Chapter III- Provisions Relating to Certain Contracts, Division I- Warranties.

[99] Ibid, section 34: "This division applies to contracts of sale or lease of goods and to contracts of service."

[100] *Ibid*, section 40.

[101] L'HEUREUX Nicole, Droit de la consommation, 5th edition, Les éditions Yvon Blais, 2000, p. 65.

Nevertheless, the companies attempt in their contracts to reduce, or at least to circumscribe the legitimate expectations of consumers. For example, on the accessibility of services at all times, the companies recall that they depend, as do consumers, on telecommunications infrastructures and that, under those conditions, it is not very realistic to expect a guarantee of constant access to those services.

Regarding warranties applicable to services, the Consumer Protection Act, S.O. 2002 provides the following in section 9(1): "*The supplier is deemed to warrant that the services supplied under a consumer agreement are of a reasonably acceptable quality.*"

The question of reasonable expectation and that of reasonably acceptable quality deserve to be discussed more thoroughly. In short, obligations may be of means or result. The obligation of means, according to Quebec doctrine, is defined by Baudouin and Jobin as "*celle pour la satisfaction de laquelle le débiteur est tenu d'agir avec prudence et diligence en vue d'obtenir le résultat convenu, en employant tous les moyens raisonnables, sans toutefois assurer le créancier de l'atteinte du résultat*[102]*.*"

The obligation of result is "*celle pour la satisfaction de laquelle le débiteur est tenu de fournir au créancier un résultat précis et déterminé*[103]*.*" The reasonable nature of consumer expectations will of course depend on the type of obligation binding the service provider. The latter is responsible for explaining, if it invokes the warranty, what were its legitimate expectations of the cloud computing service or its quality, but the courts are responsible for determining the nature of the obligation in order to judge whether the expectations are reasonable.

It should be noted that "*dans la réforme du Code civil, au chapitre du contrat d'entreprise et du contrat de service, le législateur a renoncé à fixer l'intensité de l'obligation de l'entrepreneur et du prestataire de service (sauf pour les pertes ou vices de construction des ouvrages immobiliers) : selon les circonstances de chaque espèce, le tribunal devra déterminer s'il s'agit d'une obligation de moyens ou de résultat (…)*[104]" To determine the obligation's intensity, it is necessary to "*dégager la nature de la prestation pour parvenir à la qualification appropriée*[105]*.*" One of the criteria for establishing the obligation's intensity may be whether "*l'exécution de la prestation requérait ou non une expertise professionnelle particulière : dans la négative, la conclusion d'obligation de résultat serait vraisemblable ; elle ne le serait pas, dans l'affirmative*[106]."

Cloud computing contracts contain almost systematically clauses for reducing consumers' legitimate expectations to a strict minimum, and some of those contracts provide clauses for excluding any obligation of result.

The most flagrant example of this is found in the contract of the *Dropbox* company. The clause titled "Dropbox is Available 'AS-IS'" excludes both implicit and explicit guarantees, along with those that would be related to legitimate expectations. It notably excludes guarantees of

[102] BAUDOUIN, Jean-Louis and Pierre-Gabriel JOBIN, Les Obligations, 5th edition, Éditions Yvon Blais, Cowansville, 2005, p. 37.
[103] *Ibid.*, p. 38.
[104] *Ibid.,* p. 45.
[105] LLUELLES Didier and Benoît MOORE, Droit des obligations, Les éditions Thémis, Montreal 2006, p. 45.
[106] *Ibid*., p. 45.

compliance, functionality, reliability, quality (of the service or information that the company itself can give, even setting aside the guarantee of veracity). It even provides that consent to use the service constitutes recognition that the results may be unexpected, that data may be lost or corrupted, that unforeseeable damages by the user may occur. The clause reads as follows:

> *The site, content, files and services are provided "as is", without warranty or condition of any kind, either express or implied. Without limiting the foregoing, Dropbox explicitly disclaims any warranties of merchantability, fitness for a particular purpose or non-infringement and any warranties arising out of course of dealing or usage of trade. You acknowledge that use of the site, content, file and services may result in unexpected results, loss or corruption of data or communications, project delays, other unpredictable damage or loss, or exposure of your data or your files to unintended third parties.*
>
> *Dropbox makes no warranty that the site, content, files or services will meet your requirements or be available on an uninterrupted, secure, or error-free basis. Dropbox makes no warranty regarding the quality of any products, services, or information purchased or obtained through the site, content, or services, or the accuracy, timeliness, truthfulness, completeness or reliability of any information obtained through the site, content, files or services.*
>
> *No advice or information, whether oral or written, obtained from Dropbox or through the site, content, files or services, will create any warranty not expressly made herein*[107]*.*

Unfortunately, that company is not alone in demonstrating such excess caution. For instance, *Zoho*'s contract contains the same type of clause[108].

Even Norton Online Backup, although it bills its services, provides an equally broad clause[109], although it mentions that this clause will apply only within the limits allowed by applicable laws.

Zumodrive's contract also provides a warranty exclusion clause, though more limited than the clauses mentioned above, that attempts to lower consumers' possible expectations to a realistic level: "*Company does not warrant that (i) the service will meet your specific requirements, (ii) the service will be uninterrupted, timely, or error-free, or (iii) any errors in the Service will be corrected*[110]*."*

As with waiver of liability clauses, all the major companies (*Microsoft, Google, Yahoo, Apple, Symantec* and *Facebook*) as well as *Adrive* include in their contracts mentions that warranty exclusion clauses may not apply because some jurisdictions do not allow such exclusions.

In Quebec, the Consumer Protection Act provides for a warranty that applies to goods as well as services: "40. *The goods or services provided must conform to the description made of them in the contract*" and "41. *The goods or services provided must conform to the statements or advertisements regarding them made by the merchant or the manufacturer*." Given that the legal warranty is a right that the Act grants consumers and that the Act states "261. *No person may derogate from this Act by private agreement*" and "262. *No consumer may waive the rights*

[107] Dropbox, Terms of Service [Online] http://www.dropbox.com/terms (page consulted on May 17, 2011).
[108] Zoho, Terms of Service [Online] http://www.zoho.com/terms.html (page consulted on May 17, 2011).
[109] Norton Online Backup. Terms of Service Agreement. [Online] http://www.symantec.com/content/en/us/about/media/NOBU_TOS_21_USE.pdf (page consulted on January 16, 2012).
[110] Zumodrive, Terms of Service, section 10 [Online] http://www.zumodrive.com/tos (page consulted on May 17, 2011).

granted to him by this Act unless otherwise provided herein," clauses attempting to set the legal warranty aside are inapplicable in Quebec. However, we may question whether the mention in section 19.1 is mandatory in this case, since in that section, the mention that the stipulation is inapplicable in Quebec is required only in cases where it "is inapplicable in Québec under a provision of this Act or of a regulation that prohibits the stipulation" (sec. 19.1 CPA) and that no specific section prohibits the stipulation. However, it could be argued that the general prohibition in section 261, quoted above, should entail the application of section 19.1.

In Ontario, section 9(3) of the Act of 2002 is clear – a clause intended to exclude the warranty of acceptable quality (section 9(1)) is void: "(3) *Any term or acknowledgement, whether part of the consumer agreement or not, that purports to negate or vary any implied condition or warranty under the Sale of Goods Act or any deemed condition or warranty under this Act is void*."

d) Clauses Submitting a Contract to the Application of Foreign Laws or Jurisdictions

We may legitimately ask ourselves, in the case of cloud computing contracts, what law will be applicable to the contract. Indeed, those contracts are formed at a distance, on the Internet, with foreign-based companies. The services are also rendered at a distance by those same companies. In short, nothing seems to take place where the consumer lives, where he accepts the contract terms and where he uses the service. Regarding these questions where private international law applies, the law contains certain provisions to protect consumers who enter into consumer contracts. Those provisions indicate not only the applicable law, but also the competent jurisdiction in the event of a dispute.

In Quebec, section 3117 of the Civil Code provides that:

> *The choice by the parties of the law applicable to a consumer contract does not result in depriving the consumer of the protection to which he is entitled under the mandatory provisions of the law of the country where he has his residence if the formation of the contract was preceded by a special offer or an advertisement in that country and the consumer took all the necessary steps for the formation of the contract in that country or if the order was received from the consumer in that country*[111].

In other words, a foreign court may be competent to handle a dispute between a Quebec consumer and the cloud computing service provider located abroad, but that court would have to grant the consumer the benefits to which he is entitled under Quebec law, so long as the terms of this section are met.

Under the common law, certain principles would apply; as pointed out by Michael Deturbide, for Canadian laws and jurisdictions to be competent in disputes regarding cloud computing services used by Canadian consumers:

> *The various alternatives from a consumer perspective would include reliance on Canadian jurisprudence in relation to what constitutes a "real and substantial connection" to the jurisdiction, or the application of a "jurisdiction of destination approach", or some variant thereof, in which the law and forum of the purchaser would apply to the transaction*[112].

One provision of the Consumer Protection Act reinforces the protection from which consumers benefit. Section 19 of the Act specifies "*Any stipulation in a contract that such contract is wholly*

[111] Civil Code of Québec, section 3117.
[112] DETURBIDE Michael, Consumer Protection Online, LexisNexis Butterworths, Markham, 2006, p. 30.

or partly governed by a law other than an Act of the Parliament of Canada or of the Parliament of Québec is prohibited[113]." Therefore, all cloud computing contracts concluded with Quebec consumers would necessarily be subject to Quebec laws (and clauses to the contrary should, under section 19.1 CPA, be preceded by an explicit mention confirming their inapplicability in Quebec).

In Ontario, section 100 of the Consumer Protection Act, S.O. 2002 states that "*If a consumer has a right to commence an action under this Act, the consumer may commence the action in the Superior Court of Justice*[114]." Accordingly, Ontario courts will be competent to hear lawsuits brought by Ontario consumers against cloud computing service providers, and those courts will apply this law because section 2(1) states that "*Subject to this section, this Act applies in respect of all consumer transactions if the consumer or the person engaging in the transaction with the consumer is located in Ontario when the transaction takes place*" and because section 7. (1) states that "*The substantive and procedural rights given under this Act apply despite any agreement or waiver to the contrary*."

From the above, it thus appears that cloud computing contracts are subject not only to Quebec and Ontario laws, but also that the courts of these provinces are competent to hear lawsuits that might arise following the conclusion of those cloud computing contracts.

However, these provisions do not prevent almost all cloud computing contracts from providing, in the event of disputes, the application of foreign laws and from considering foreign courts to be competent to take decisions in such disputes, and occasionally those contracts even explicitly set aside the rules of legal disputes that should apply for deciding on these matters as need be.

For example, section 20.7 of Google's terms of use mentions "*The Terms, and your relationship with Google under the Terms, shall be governed by the laws of the State of California without regard to its conflict of laws provisions. You and Google agree to submit to the exclusive jurisdiction of the courts located within the county of Santa Clara, California to resolve any legal matter arising from the Terms.*"

It should be pointed out that the consumer cannot waive a right conferred to him by the Consumer Protection Act[115], or the Consumer Protection Act, S.O. 2002[116]. The fact that the clauses in question imply that the consumer "pledges" can thus have no legal effect. Nor can the merchant contractually unilaterally remove the consumer's rights under those laws[117]. The consumer thus cannot waive the application of section 19 of the Consumer Protection Act or of section 100 of the Consumer Protection Act, S.O. 2002.

[113] Consumer Protection Act, R.S.Q., chapter P-40.1, section 19.
[114] Consumer Protection Act, S.O. 2002, S.O. 2002, chapter 30, section 100.
[115] Consumer Protection Act, R.S.Q., chapter P-40.1, section 262.
[116] Consumer Protection Act, S.O. 2002, S.O. 2002, chapter 30, section 7.
[117] Consumer Protection Act, R.S.Q., chapter P-40.1, section 261 and Consumer Protection Act, S.O. 2002, S.O. 2002, chapter 30, section 7.(1).

The contracts of *Apple*'s "*MobileMe*"[118], *Facebook*[119] and *Norton Online Backup*[120] provide that the laws of the State of California will apply to the contractual relation with consumers, and that the competent court will be that of Santa Clara. The companies *Adrive*[121] and *Dropbox*[122] also provide the application of California laws, but designate as competent the court of San Francisco.

The only two companies that do not refer to the laws of the state where they have their head office, or to the courts in those locations, are *Microsoft* and *Yahoo!*. In fact, *Microsoft* provides that the applicable laws are those of the consumer's place of residence: "*All other claims, including claims regarding consumer protection laws, unfair competition laws, and in tort, will be subject to the laws of your state of residence in the United States, or, if you live outside the United States, the laws of the country to which we direct your service*[123]."

Ontario consumers who use Yahoo! Services benefit from preferential treatment: section 26 des of *Yahoo!*'s terms of use stipulate that "*The TOS and the relationship between you and Yahoo! shall be governed by the laws of the province of Ontario and Canada without regard to its conflict of law provisions. You and Yahoo! agree to submit to the personal and exclusive jurisdiction of the courts located within the province of Ontario, Canada*[124]." Consumers from other province will have to invoke the common law or provincial consumer protection laws for the courts and laws of their provinces to apply to their contractual relationship. Quebec consumers will invoke section 19 of the consumer Protection Act.

Finally, apart from companies whose silence suggests a recognition that Canadian laws would apply to their relations with Canadian consumers, and apart from Microsoft, which recognizes the competence of Canadian courts and laws, all the other companies appear to want to ignore the laws that, by imposing the competence of provincial courts and the application of provincial laws in consumer contracts, aim to protect consumers.

e) Arbitration Clauses

The consumer protection laws of Ontario and Quebec are clear: mandatory arbitration cannot be imposed on consumers by means of provisions (called arbitration clauses) contained in consumer contracts covered by those laws.

[118] MobileMe, Terms of Service, section 16 [Online] http://www.apple.com/legal/mobileme/fr/terms.html (page consulted on May 17, 2011).
[119] Facebook, Statement of Rights and Responsibilities, section 15. [Online] http://www.facebook.com/terms.php?ref=pf (page consulted on May 17, 2011).
[120] Norton Online Backup. Terms of service agreement. [Online] http://www.symantec.com/content/en/us/about/media/NOBU_TOS_21_USE.pdf (page consulted on January 16, 2012). A general provision of Symantec's Terms of Service Agreement nevertheless states that the terms of the agreement do not supersede the user's national laws, if those laws do not allow it (section 17).
[121] Adrive, Terms of Service, section 20 [Online] http://www.adrive.com/terms (page consulted on May 17, 2011).
[122] Dropbox, Terms of Service [Online] http://www.dropbox.com/terms (page consulted on May 17, 2011).
[123] Microsoft, Service Contract, section 13, [Online] http://explore.live.com/microsoft-service-agreement?ref=none (page consulted on May 17, 2011).
[124] Yahoo!, Terms of Use, section 26 [Online] http://info.yahoo.com/legal/ca/yahoo/utos/utos-ca01.html (page consulted on May 17, 2011).

Section 11.1 of the Consumer Protection Act provides that "*Any stipulation that obliges the consumer to refer a dispute to arbitration, that restricts the consumer's right to go before a court, in particular by prohibiting the consumer from bringing a class action, or that deprives the consumer of the right to be a member of a group bringing a class action is prohibited*[125]." It should be noted that a clause that would prohibit processing a dispute collectively (or that would thus impose individual processing) is also prohibited (and that, if a contract intended for Quebec consumers contained such a clause, it should, under section 19.1 CPA, be preceded by an explicit mention confirming its inapplicability in Quebec).

In that vein, section 7(2) of the Consumer Protection Act, S.O. 2002 stipulates that "*any term or acknowledgment in a consumer agreement or a related agreement that requires or has the effect of requiring that disputes arising out of the consumer agreement be submitted to arbitration is invalid insofar as it prevents a consumer from exercising a right to commence an action in the Superior Court of Justice given under this Act*[126]."

However, although the arbitration clause is prohibited in Quebec and invalid in Ontario, we find this type of clause in some cloud computing contracts.

This is notably the case in *Zoho* and *Adrive* contracts.

The clauses of those contracts have the same effect, so we only quote section 25 of *Adrive*'s terms of use, which, like the corresponding section in *Zoho*'s contract[127], imposes arbitration as well as individual handling of disputes to come:

> *Any dispute between you and Adrive relating to this Agreement, Storage Data or Adrive's services, hardware or software shall be resolved by binding arbitration pursuant to the commercial rules of the American Arbitration Association. Any such controversy or claim shall be arbitrated on an individual basis, and shall not be consolidated in any arbitration with any claim or controversy of any other party. The arbitration shall be conducted in San Francisco, California, and any judgment on the arbitration award may be entered in any court having jurisdiction thereof*[128].

We recall that the Supreme Court of Canada decided in 2007, in the Dell case[129], in favour of arbitration in consumer affairs and, listing the benefits of arbitration, refused to recognize that imposing an arbitration clause and prohibiting class actions constituted a consumer's waiver of the competence of Quebec authorities – an invalid waiver under the Civil Code of Quebec (sec. 3148 and 3149). The Government of Quebec – the province where the case originated –reacted quickly (even before the ruling was made in this case) by explicitly prohibiting arbitration clauses in contracts covered by the CPA.

Recently, the Supreme Court of Canada has ruled again, in the *Seidel v. Telus Communications Inc.* case, originating in British Columbia, regarding arbitration in consumer affairs.

[125] Consumer Protection Act, R.S.Q., chapter P-40.1, section 11.1.
[126] Consumer Protection Act, S.O. 2002, S.O. 2002, chapter 30, section 7(2).
[127] Zoho, Terms of Service [Online] http://www.zoho.com/terms.html (page consulted on May 17, 2011).
[128] Adrive, Terms of Service, section 25 [Online] http://www.adrive.com/terms (page consulted on May 17, 2011).
[129] Dell Computer Corp. v. Union des consommateurs, [2007] 2 S.C.R. 801, 2007 SCC 34.

> *[5] Section 172 of the BPCPA contains a remedy whereby "a person other than a supplier, whether or not the person bringing the action has a special interest or any interest under this Act or is affected by a consumer transaction that gives rise to the action, may bring an action in Supreme Court" to enforce the statute's consumer protection standards. Under s. 3 of the BPCPA, any agreement between the parties that would waive or release "rights, benefits or protections" conferred by the BPCPA is "void". My opinion is that to the extent Ms. Seidel's claim in the Supreme Court invokes s. 172 remedies in respect of "rights, benefits or protections" conferred by the BPCPA, her court action must be allowed to proceed notwithstanding the mediation/arbitration clause*[130].

The decision recalls the reasons why consumer protection laws limit or prohibit mandatory arbitration clauses:

> *[24] Nevertheless, from the perspective of the [Business Practices and Consumer Protection Act]* BPCPA, *"private, confidential and binding arbitration" will almost certainly inhibit rather than promote wide publicity (and thus deterrence) of deceptive and/or unconscionable commercial conduct. It is clearly open to a legislature to utilize private consumers as effective enforcement partners operating independently of the formal enforcement bureaucracy and to conclude that the most effective form is not a "private and confidential" alternative dispute resolution behind closed doors, but very public and well-publicized proceedings in a court of law*[131].

However, we observe that mandatory arbitration is but an epiphenomenon among the cloud computing contracts studied, since only two contracts contain arbitration clauses. This practice is thus apparently fading.

f) Unilateral Alteration and Termination Clauses

The clauses whose presence we wanted to verify in contracts allow companies providing cloud computing services to alter at will the contract binding them to consumers or to terminate it unilaterally.

We determined above that cloud computing contracts corresponded to the characterization of contracts of successive performance for a service provided at a distance. For this type of contract, the Consumer Protection Act provides in section 11.3 rules for merchants' unilateral alteration or for clauses allowing it:

> *Any stipulation under which the merchant may unilaterally cancel a fixed-term service contract involving sequential performance is prohibited, except under articles 1604 and 2126 of the Civil Code and, in the latter case, only in accordance with article 2129 of the Code. A merchant who intends to cancel an indeterminate-term service contract involving sequential performance must notify the consumer in writing at least 60 days before the date of cancellation if the consumer has not defaulted on his obligation*[132].

[130] Seidel v. TELUS Communications Inc., 2011 SCC 15.
[131] Seidel v. TELUS Communications Inc., 2011 SCC 15.
[132] However, Quebec's law allows consumers to terminate such a contract at any time: Civil Code of Québec: "*2125. The client may unilaterally resiliate the contract even though the work or provision of service is already in progress*." (Section 2129 mentions the amounts that customers might have to pay.) Consumer Protection Act, R.S.Q., chapter P-40.1, section 214.6: "*The consumer may, at any time and at the consumer's discretion, cancel the contract by sending a notice to the merchant. The cancellation takes effect by operation of law on the sending of the notice or the date specified in the notice*."

The Act thus provides two types of prescriptions for unilateral alteration clauses, whether the contract is fixed-term or open-ended. We find cloud computing contracts in both these categories. Some cloud computing contracts – those that impose subscription or usage fees – are fixed-term, with the consumer pledging to pay for the service in the definite period – whether months or years – during which he will obtain the service. The CPA prohibits the merchant from reserving the right to terminate the contract for any reason other than non-payment (1604 C.C.Q.) or any other serious reason (2126 C.C.Q.) and, in that case, only if the clause provides that the consumer will be reimbursed any overpayment (2129 C.C.Q.).

"Free" cloud computing contracts are open-ended contracts; some contracts provide the company's account termination in the event of extended non-use of the service. The only obligation imposed by the Act is to notify the user 60 days before termination.

Regarding unilateral alterations of contracts, section 11.2 of the Consumer Protection Act strictly regulates this type of clause:

> *Any stipulation under which a merchant may amend a contract unilaterally is prohibited unless the stipulation also:*
> *a) specifies the elements of the contract that may be amended unilaterally;*
> *b) provides that the merchant must send to the consumer, at least 30 days before the amendment comes into force, a written notice drawn up clearly and legibly, setting out the new clause only, or the amended clause and the clause as it read formerly, the date of the coming into force of the amendment and the rights of the consumer set forth in subparagraph c; and;*
> *c) provides that the consumer may refuse the amendment and rescind or, in the case of a contract involving sequential performance, cancel the contract without cost, penalty or cancellation indemnity by sending the merchant a notice to that effect no later than 30 days after the amendment comes into force, if the amendment entails an increase in the consumer's obligations or a reduction in the merchant's obligations.*
>
> *However, except in the case of an indeterminate-term service contract, such a stipulation is prohibited if it applies to an essential element of the contract, particularly the nature of the goods or services that are the object of the contract, the price of the goods or services or, if applicable, the term of the contract*[133]*.*

In Ontario, section 13(4) de la Consumer Protection Act, S.O. 2002 specifies that "*If a consumer is receiving goods or services on an ongoing or periodic basis and there is a material change in such goods or services, the goods or services shall be deemed to be unsolicited from the time of the material change forward unless the supplier is able to establish that the consumer consented to the material change*."

Under section 13(5), the consumer's consent may be given verbally, in writing or by any other positive action. The provisions of the applicable regulation indicate what is meant by "material change:" "*a change or a series of changes is a material change if it is of such nature or quality that it could reasonably be expected to influence a reasonable person's decision as to whether to enter into the agreement for the supply of the goods or services*[134]." Amendments, renewal or extension of some consumer agreements, including Internet agreements and agreements of

[133] Consumer Protection Act, section 11.2.
[134] Ontario Regulation 17/05, section 20.[135] Ontario Regulation 17/05, section 42. (5): "*The supplier's notice of a proposal to amend, renew or extend shall,*

successive performance, are covered by sections 41 and 42 of the Consumer Protection Act, S.O. 2002 Regulation. Sections 41(2) and 41(3) provide the following:

> (2) *A consumer agreement mentioned in subsection (1), whether it provides for amendment, renewal or extension or not, may be amended, renewed or extended if*:
> a) *the supplier or the consumer makes a proposal for amendment, renewal or extension ;*
> b) *the supplier provides to the consumer an update of all of the information that was required by the Act or this Regulation to be set out in the agreement when it was first entered into and the update reflects the effect of the proposal to amend, renew or extend; and*
> c) *the party who receives the proposal agrees, explicitly and not merely by implication, to the proposal*.
>
> (3) *For the purpose of clause (2) (c), an acknowledgement that the proposal has been received does not in itself constitute agreement to the proposal*.

Clauses granting the merchant the right to amend the contract are covered in section 42 of the Regulation:

> 42. (2) *A consumer agreement mentioned in subsection (1) that provides for amendment, renewal or extension may, in addition to being amendable, renewable or extendable under section 41, be amended, renewed or extended if the following conditions are satisfied*:
> 1. *The agreement indicates what elements of the agreement the supplier may propose to amend, renew or extend and at what intervals the supplier may propose an amendment, renewal or extension*.
> 2. *The agreement gives the consumer at least one of the following alternatives to accepting the supplier's proposal to amend, renew or extend*:
> i. *terminating the agreement, or*
> ii. *retaining the existing agreement unchanged*.
> 3. *The agreement requires the supplier to give the consumer advance notice of a proposal to amend, renew or extend*.
>
> 42. (3) *The amendment, renewal or extension takes effect on the later of,*
> a) *the date specified in the notice; and*
> b) *the date that is 30 days after the day on which the consumer receives the notice*.

The notice of the proposal to amend, renew or extend the contract must also comply with the characteristics provided in section 42(5) of the Regulation[135], failing which it will be invalid.

Now that the legal framework is determined, we will attempt to find, in the cloud computing contracts we have selected, examples of amendment clauses.

We will classify contracts in two categories: fix-term and open-ended. For each category, we will examine the compliance of clauses with Quebec laws.

Fixed-term contracts
In the first category are the fixed-term contracts of *MobileMe, Dropbox, Zoho, Zumodrive,* and *Adrive*.

In the *Adrive* contract, section 18 reserves to the company the right to amend the contract unilaterally and the right to terminate the contract at any time.[136]

In that vein, *Zumodrive* reserves the right to alter the service without notifying users; the simple fact of the user continuing to use the service will constitute consent to such an alteration. The only mention of a notice in the event of amendment concerns the service's rates; 30 days' notice before the change will be sent to the user. Moreover, the company reserves the right to terminate the service at its own discretion[137].

Dropbox's contract also contains clauses regarding unilateral contract alteration and service termination. Thus, the company may terminate the service at its sole discretion and change service access and usage[138].

The *MobileMe* contract contains a clause allowing Apple to terminate the service unilaterally[139] and change the price unilaterally: "*Apple may at any time, upon notice required by applicable law, change the price of the Service or any part thereof, or institute new charges or fees*[140]." Under the terms of the contract, the user's continuing to use the service will mean his consent to the price change[141].

Zoho reserves the right to alter the service unilaterally at any time; but the company will notify users (by means of a notice or a publication on the website) at the moment when the contract amendment is made[142].

For its part, the service *Norton Online Backup*, which *Symantec* bills on an annual basis, nevertheless provides in section 8 a right of amendment that mentions no prior notice:

[136] Adrive, Service Agreement, section 18 [Online] http://www.adrive.com/terms (page consulted on May 17, 2011).
[137] Zumodrive, Terms of Service [Online] http://www.zumodrive.com/tos (page consulted on May 17, 2011).
[138] Dropbox, Terms of Service: "*These Terms of Service limit Dropbox's liability and obligations to you, grant Dropbox certain rights and allow Dropbox to change, suspend or terminate your access to and use of the Site, Content, Files and Services.*" [Online] http://www.rogerclarke.com/EC/IU-SPE-T-Dropbox.html (page consulted on May 17, 2011).
[139] MobileMe, Terms of Service, section 10 [Online] http://www.apple.com/legal/mobileme/en/terms.html (page consulted on May 17, 2011).
[140] *Ibid.*
[141] MobileMe, Terms of Service, section 6 [Online] http://www.apple.com/legal/mobileme/en/terms.html (page consulted on May 17, 2011).
[142] Zoho, General Terms of Service [Online] http://www.zoho.com/terms.html (page consulted on May 17, 2011).

> *8. [...] In order to optimize the Software and Service Symantec may, at its discretion and without notice, add, modify or remove features from the Software or Service at any time. In such event, you may be required to upgrade to the latest version of the Software in order for the Service to continue to function correctly. You agree that Symantec may, in its sole discretion and from time to time, establish or amend general operating practices to maximize the operation and availability of the Service and to prevent abuses*[143].

We observe that none of the contracts examined complies with the provisions of sections 11.2 and 11.3 of the Consumer Protection Act, or with the requirements of sections 41(2) and 42(2) of the Consumer Protection Act, S.O. 2002 Regulation.

Contract amendment clauses

As mentioned above, under CPA section 11.2, stipulations that allow merchants to amend a contract unilaterally de la CPA are prohibited, unless such stipulations also specify which elements could be amended.

In addition to the fact that the merchant must notify the consumer in writing at least 30 days before the effective date of the amendment, by sending him the amended clause and the previous version (or the new clause, in case of an addition), the amendment clause must mention it, as well as the consumer's right to refuse the amendment and terminate the contract if the amendment increases his obligation or reduces the merchant's obligation.

Section 11.2 also provides that the merchant cannot, in the case of an open-ended contract, reserves the right to amend an essential element of the contract (nature of the good or service, price, term of the contract).

While the mention of a notice to be sent is already exceptional in amendment clauses found in aux cloud computing contracts, those that are found there do not meet the CPA's conditions – neither in prohibiting the amendment of a material element of the contract, nor even in mentioning the elements of the contract that could be so amended.

In addition, no mention is made about the possibility for the consumer to terminate the contract if he refuses such an amendment.

Despite the CPA's express prohibition, some companies candidly announce that they reserve the right to change the price of the services unilaterally. Since those clauses, which do not meet the conditions of CPA section 11.2, they should, under CPA section 19.1, be preceded by an explicit mention confirming their inapplicability in Quebec – a mention that companies including the prohibited clauses neglect to insert.

Those unilateral amendment clauses also do not meet the conditions imposed by sections 42(2) and 42(3) of the Consumer Protection Act, S.O. 2002 Regulation, which also provides the obligation to indicate the elements a company reserves the right to amend; the consumer's right to terminate the agreement or maintain it unchanged; and the company's obligation "*to give the consumer advance notice of a proposal to amend, renew or extend*."

[143] Norton Online Backup. Terms of service agreement. [Online] http://www.symantec.com/content/en/us/about/media/NOBU_TOS_21_USE.pdf (page consulted on January 16, 2012).

Unilateral termination clause

Some companies reserve the right to terminate the service at their sole discretion, while section 11.3 of the Consumer Protection Act limits the possibilities of the contract being terminated unilaterally, except under sections 1604, 2126 and 2129 of the Civil Code of Québec. Under section 1604 of the Civil Code of Québec, as Vincent Karim points out:

> *dans le cas d'une inexécution partielle, le créancier n'aura droit à la résiliation du contrat que si le défaut du débiteur est répété. Ainsi, une faute mineure qui se produit de façon continuelle et constante peut constituer un défaut important. Un créancier ne peut invoquer les manquements du débiteur pour se libérer de ses obligations corrélatives, à moins que ces manquements ne revêtent le caractère répétitif exigé par la Loi*[144].

With regard to section 2126 of the Civil Code of Québec, the Justice Minister specifies that this section:

> *accorde un droit de résiliation unilatérale plus circonscrit que celui reconnu au client, puisqu'il doit être justifié par un motif sérieux et ne doit pas être exercé à contretemps. En cas de résiliation, le prestataire de service (…) doit, en plus, prendre tous les moyens pour prévenir une perte ; il doit veiller, même au moment de la résiliation, à la protection immédiate des intérêts du client*[145].

Moreover, under section 2129 of the Civil Code of Québec, "*the contractor or the provider of services is bound to repay any advances he has received in excess of what he has earned.*"

[144] KARIM Vincent, Les obligations, Volume 2, Wilson & Lafleur Ltée, 2009, pp.599-600

[145] BAUDOUIN Jean-Louis and Yvon Renaud, Code civil du Québec annoté, Wilson Lafleur, 12th edition, 2009, Tome 2, p. 3036.

Open-ended contracts
Among open-ended contracts are those of *Yahoo!,* whereby the company reserves the right to amend the contract without prior notice, and to terminate the contract at its discretion[146].

Microsoft's contract mentions that the company may amend the contract, but that a notice will be sent to the user; however, the contract does not indicate a period for notifying the consumer, who may terminate the service if he refuses the amendment. It should be noted that the company may terminate the service without a notice[147].

For *Google's* services, the terms of use reserve to the company the right to terminate the service unilaterally; the company also reserves the right to amend the contract by announcing the amendments on its website, but without sending users a notice. Simply using the services implies acceptance of its alterations[148].

MobileMe, Zoho, Zumodrive and *Adrive* contain similar provisions. The following comments and observations will therefore apply to the contracts of those companies as well.

Contract amendment clauses
Again, we note that companies do not comply with the provisions of the Consumer Protection Act. Some companies do not provide for sensing a contract amendment notice, and those that do so do not indicate that they will comply with the form of the notice as prescribed in section 11.2 of the Consumer Protection Act.

Unilateral amendment clause
As part of such open-ended service contracts of successive performance, the company is obliged to send a written notice at least 60 days before the contract termination date. This is the only requirement imposed on companies. Nothing indicates that they plan to comply with it.

g) Automatic Subscription Renewal Clauses

The Consumer Protection Act, in contrast with the Consumer Protection Act, S.O. 2002, contains certain provisions for automatic contract renewals.

Thus, CPA section 214.3[149] prohibits contractual clauses to automatically renew a contract of over 60 days upon the end of the term, except for an indeterminate period. Moreover, section 214.4 of the Act requires that a notice be sent to the consumer 90 to 60 days before the end of the contract, in order to inform him of the contract's expiry date.

Of all the open-ended contracts examined, the only one containing a renewal clause is that of *MobileMe,* in section 6:

[146] Yahoo!, Terms of Use, section 13 [Online] http://info.yahoo.com/legal/ca/yahoo/utos/utos-ca01.html (page consulted on May 17, 2011).
[147] Microsoft, Service Contract, section 8 [Online] http://explore.live.com/microsoft-service-agreement?ref=none (page consulted on May 17, 2011).
[148] Google, Terms of Service, Section 13.3 [Online] http://www.google.com/accounts/TOS (page consulted on May 17, 2011).
[149] Consumer Protection Act, R.S.Q., chapter P-40.1, section 214.3: "*Any stipulation under which a contract whose term exceeds 60 days is renewed upon its expiry is prohibited, unless the renewal is for an indeterminate term.*"

> *When you sign up online for the Service, your annual subscription will be set to automatically renew upon its expiration. This means that unless you cancel your account or change its renewal settings prior to its expiration, your account will automatically renew for another year. At the time of renewal, we will charge your credit card the then-current fees to renew the Service. About thirty (30) days prior to your expiration date we will notify you by email to your MobileMe email address that your account is about to renew and remind you that your credit card will be billed the indicated Service fees on the renewal date. You may change your renewal settings at any time by going to https://secure.me.com/account.*

Thus, this section complies neither with the rules stated in section 214.3 nor with the period prescribed in section 214.4 of the CPA. In fact, the *MobileMe* contract provides a renewal for a similar period to that provided initially, whereas the contract should, upon maturity, become an open-ended contract. Because a clause of this type that does not comply with section 214.3 is prohibited, an explicit and evident mention should, under CPA section 19.1, precede that clause to indicate that it is inapplicable in Quebec.

h) Conclusion

This analysis of cloud computing contracts in the light of consumer protection laws reveals that those contracts often ignore the provisions of those laws. It can therefore be expected that if the contracts are not amended in the future, the courts will have to examine them after frustrated consumers complain or consumer protection authorities investigate.

The scope and effects of those contractual clauses should be examined from consumers' viewpoint and legally. The reason why certain clauses are prohibited and that, in Quebec, the legislators want their inapplicability to be expressly mentioned to consumers, is that the latter, if poorly informed, could be misled by those clauses: indeed, as is often said, the contract is the law of the parties. In consumer contracts, this rule is not always true: a public policy statute causes certain laws to considered unwritten. It remains for the consumer to know precisely which of the many clauses of his contract should be disregarded… The provisions of consumer protection laws notably aim to prevent companies from taking advantage of consumers' vulnerability. Including in contracts clauses that should not be there constitute just such an abuse: the consumer is led to believe that he has less rights than he does in reality.

5.2 Remedies Available to Consumers and Sanctions Applied when Consumer Protection Laws Are Violated

Again, because the Consumer Protection Act is a public policy statute, Quebec consumers generally cannot waive a right it confers to them[150] (nor the merchant deprive them of such a right). Although the contract is the law of the parties, the provisions of the consumer Protection Act cannot be set aside by one or more contractual clauses[151]. The Consumer Protection Act, S.O. 2002 has adopted a similar principle in its section 7[152].

Generally, clauses contravening the provisions of consumer protection laws will be inapplicable to consumers – for instance, arbitration clauses, waiver of liability clauses, clauses submitting the contract to foreign laws or jurisdictions. Certain sections of the CPA expressly establish this principle. For example, section 11.2, on unilateral amendments to contracts, indicates that "*Any amendment of a contract in contravention of this section cannot be invoked against the consumer* [153]." CPA sections 271 and 272 provide that infractions of contract formation rules allow the consumer to demand the contract's invalidity, and that the merchant's default to his obligations under the Act may entail the invalidity, rescission or termination of the contract, and a reduction of the consumer's obligations, without prejudice to damages to which he may be entitled or to punitive damages he may claim.

We recall the terms of the contracts of *Dropbox*, *Symantec* and *Adrive*, which can amend the terms of service and even the price of the service. Under those conditions, according to CPA section 11.2, those amendments could not be invoked against the consumer. Similarly, the consumer may avail himself of the remedies provided by CPA sections 271 and 272, and terminate the service.

In Ontario, in case of an infraction of contract amendment rules as defined in the Consumer Protection Act, S.O. 2002 Regulation, consumers have the right to terminate the agreement or maintain it unchanged. Section 93 of the Act specifies that "*A consumer agreement is not binding on the consumer unless the agreement is made in accordance with this Act and the regulations.*" But subsection 2 of this section provides that "*Despite subsection (1), a court may order that a consumer is bound by all or a portion or portions of a consumer agreement, even if the agreement has not been made in accordance with this Act or the regulations, if the court determines that it would be inequitable in the circumstances for the consumer not to be bound*[154]." Consumers may thus demand the termination of contracts containing arbitration clauses or submit he contract to the application of foreign laws or jurisdictions. As for other problematic clauses, the remedies of Ontario consumers must be based on the theory of "unconscionable practices," particularly to oppose waiver of liability clauses.

[150] *Ibid.*, section 262: "*No consumer may waive the rights granted to him by this Act unless otherwise provided herein.*"
[151] *Ibid*, section 261: "*No person may derogate from this Act by private agreement.*"
[152] *Consumer Protection Act, S.O. 2002, chapter 30*, section 7: "*The substantive and procedural rights given under this Act apply despite any agreement or waiver to the contrary*."
[153] *Consumer Protection Act, R.S.Q., chapter P-40.1,*section 11.2.
[154] On the application of this section, see the decision on Weller v. Reliance Home Comfort Limited Partnership, 2011 ONSC 3148.

Quebec law considers a clause to be abusive if it "*An abusive clause is a clause which is excessively and unreasonably detrimental to the consumer or the adhering party and is therefore not in good faith; in particular, a clause which so departs from the fundamental obligations arising from the rules normally governing the contract that it changes the nature of the contract is an abusive clause*[155]." In a consumer contract, such a clause is null or "*the obligation arising from it may be reduced*[156]."

Some of the clauses of cloud computing contracts could likely be considered abusive, such as indemnity clauses imposed on consumers for free services. We think there is a disproportion when companies disclaim any responsibility while the service is said to be free[157]. Section 8 of the Consumer Protection Act provides the following:

> *The consumer may demand the nullity of a contract or a reduction in his obligations thereunder where the disproportion between the respective obligations of the parties is so great as to amount to exploitation of the consumer or where the obligation of the consumer is excessive, harsh or unconscionable*[158].

As opposed to clauses that Quebec law would characterize as abusive, Ontario consumers would have to prove that they are "unconscionable." Section 18 (1) of the Consumer Protection Act, S.O. 2002 clearly states the sanction for this type of practice: "*Any agreement, whether written, oral or implied, entered into by a consumer after or while a person has engaged in an unfair practice may be rescinded by the consumer and the consumer is entitled to any remedy that is available in law, including damages.*" Subsection 11 also provides that "*A court may award exemplary or punitive damages in addition to any other remedy in an action commenced under this section.*"

In all cases, consumers must go to court to assert their rights. In Quebec, the Small Claims Division, which can receive requests not exceeding $7,000, will likely be the appropriate court[159]. In Ontario, the maximum amount in the Small Claims Court cannot exceed $25,000[160]. Again, consumers can often obtain cloud computing services without having to pay any money – in other words, the ceilings should not limit consumers' remedies, unless consumers claim damages exceeding those ceilings.

Given that the amounts of money at play, at least in terms of fees for using cloud computing services, appear quite low, we may ask whether consumers will go to court to assert their rights if cloud computing companies infringe them. The question is worthwhile since proceedings initiated by consumers against cloud computing services will entail costs (direct and indirect) for consumers. Experience shows that, for a consumer to go to court, the damages caused by a company have to be substantial enough for the cost-benefit calculation to justify the initiative. However, the circumstances where damages suffered by a consumer might be high seem to us quite infrequent. Still, given that cloud computing contracts are adhesion contracts, it can be expected that one consumer's reproach (and reason for claiming damages) would also be that of many users. The class action initiated against Facebook probably shows path to be taken if disputes regarding cloud computing services deserve to be taken to court.

[155] Civil Code of Québec, section 1437 subsection 2.
[156] *Ibid*, subsection 1.
[157] Read in particular the contract provisions of Dropbox and Facebook.
[158] *Consumer Protection Act, R.S.Q., chapter P-40.1*, section 8.
[159] Code of Civil Procedure, R.S.Q., c-25, section 953.
[160] Ontario Regulation 626/00, Small Claims Court Jurisdiction and Appeal Limit.

Governmental organizations responsible for applying consumer protection laws have the power to initiate criminal proceedings against delinquent companies. Consumers may therefore also complain to those authorities in order to have sanctions imposed.

In Quebec, the Office de la protection du consommateur (OPC) has "*the duty of the Office to protect consumers and, to that end, a) to supervise the application of this Act (…); b) to receive complaints from consumers*[161]." So consumers may complain to the OPC about the contractual practices of cloud computing companies and about the presence in contracts of clauses violating the Consumer Protection Act. The OPC President has certain powers under those circumstances, as stated in CPA section 316; the President may request that the court issue an injunction ordering the cloud computing company to stop inserting a stipulation prohibited in Quebec or to precede it by the mention of inapplicability provided in CPA section 19.1. In short, CPA section 316 also allows a consumer protection organization to request this type of injunction.

In Ontario, there are no similar provisions regarding inapplicable clauses. However, consumers may also complain before the Department[162]. The Director has a power of order to force companies to observe the law[163]; the Director is "*the person designated as the Director under the Ministry of Consumer and Business Services Act*[164]."

[161] *Consumer Protection Act, R.S.Q., chapter P-40.1,* section 292.

[162] Consumer Protection Act, S.O. 2002, S.O. 2002, chapter 30, section 105: "*The Ministry may:*
a) receive complaints concerning conduct that may be in contravention of this Act, of other legislation for the protection of consumers or of any other prescribed Act, whether the conduct constitutes an offence or not; and;
b) make inquiries, gather information and attempt to mediate or resolve complaints, as appropriate, concerning any matter that comes to its attention that may be in contravention of this Act, of other legislation for the protection of consumers or of any other prescribed Act, whether the matter constitutes an offence or not."

[163] Consumer Protection Act, S.O. 2002, S.O. 2002, chapter 30, section 111: "(1) *The Director may propose to make an order directing a person to comply with the Act if the Director believes on reasonable grounds that the person has engaged or is engaging in any activity that contravenes any provision under this Act, whether the activity constitutes an offence or not.*"

[164] *Ibid.* Note 163, section 1.

6 Analysis of Cloud Computing Provisions in the Light of the Copyright Act

While, as our research indicates, cloud computing contracts are problematic according to consumer protection laws, they may be so in the light of the Copyright Act as well.

One of the attractions of cloud computing services is that they allow users to share, and even to create contents of all kinds. The *Flickr* service, for example, enables users to share photos taken by the person putting them online or by a third party. Other cloud computing services, such as *Facebook*, make it possible to share not only photos, but also comments. Online text editors such as *Google docs* and *Zoho* enable the creation of documents to be stored and shared online. Most storage services also make it possible for users to share documents; this is notably the case with *Adrive*, *Dropbox* and *Zumodrive*.

Of course, questions may be raised about the property of works thus created, shared or stored online, and about usage rights normally reserved for an author or creator.

> Normand Tamaro writes as follows about the "property right" conferred to an author by the Copyright Act with regard to his works:
>
> *[…] la Cour suprême, dans l'affaire Bishop, relevait que la Loi sur le droit d'auteur a un but unique et a été adoptée au seul profit des auteurs de toutes sortes, que leurs œuvres soient littéraires, dramatiques ou musicales.*
>
> *Pour notre plus haut tribunal, la Loi sur le droit d'auteur est donc de la nature d'un droit de propriété accordé aux auteurs en vertu des principes de justice naturelle en retour d'une propriété qu'ils ont eux-mêmes créée. En effet, à la différence de la personne qui acquiert un droit sur un bien qui préexiste, par exemple la personne qui achète un immeuble, c'est précisément par le fait de l'auteur que le droit d'auteur existe. L'auteur est la condition sine qua non de l'existence du droit. Sans l'œuvre de l'auteur, il n'y a pas de droit d'auteur. […]*
>
> *Le droit d'auteur est donc un droit de propriété privé portant sur un bien, une œuvre, qui ne préexistait pas à son auteur, et qui ne prive personne de quoi que ce soit, sauf de la liberté de s'emparer de ce qu'un auteur a exprimé sous une forme qui lui est originale*[165].

Under section 5 of the Copyright Act: *Works in Which Copyright May Subsist*, this right is granted to the creator of an original literary, dramatic, musical or artistic work.

> *"every original literary, dramatic, musical and artistic work" includes every original production in the literary, scientific or artistic domain, whatever may be the mode or form of its expression, such as compilations, books, pamphlets and other writings, lectures, dramatic or dramatico-musical works, musical works, translations, illustrations, sketches and plastic works relative to geography, topography, architecture or science*[166].

[165] TAMARO Normand, Loi sur le droit d'auteur, 6th edition, Thomson Carswell, Scarborough, Ontario, 2003, p. 3.
[166] Copyright Act, RSC 1985, c C-42, section 2, Definitions.

Originality, the essential condition for copyright, as defined by the Supreme Court in the *CCH Canadian Limited v. Law Society of Upper Canada* decision:

> *An "original" work under the Copyright Act is one that originates from an author and is not copied from another work. In addition, an original work must be the product of an author's exercise of skill and judgment*[167].

The creator of an original work has "*the sole right to produce or reproduce the work or any substantial part thereof in any material form whatever, to perform the work or any substantial part thereof in public or, if the work is unpublished, to publish the work or any substantial part thereof (…)*[168]." Section 3 draws a long list of exclusive rights, including that of transforming, adapting, translating the work, and of communicating it to the public by telecommunications.

The author also has moral rights: "*The author of a work has, subject to section 28.2, the right to the integrity of the work and, in connection with an act mentioned in section 3, the right, where reasonable in the circumstances, to be associated with the work as its author by name or under a pseudonym and the right to remain anonymous*[169]*."*

Under section 13(4) of the Copyright Act:

> *The owner of the copyright in any work may assign the right, either wholly or partially, and either generally or subject to limitations […], either for the whole term of the copyright or for any other part thereof, and may grant any interest in the right by licence, but no assignment or grant is valid unless it is in writing signed by the owner of the right in respect of which the assignment or grant is made, or by the owner's duly authorized agent*[170].

The distinction between assigning rights and a simple licence allowing their use is important. Indeed, by assigning rights, the author sells part or all of his economic rights. A licence, on the other hand, is equivalent to the owner leasing his rights: the author allows the licensee to use some or all the copyright, but retains ownership of the work.

> *La cession de droit : il s'agit d'un transfert de propriété relatif à l'un ou plusieurs des droits économiques liés au droit d'auteur sur l'œuvre (ou de l'un des droits exclusifs conférés à l'artiste-interprète, au producteur d'un enregistrement sonore ou au radiodiffuseur). Soulignons que la cession du droit d'auteur n'emporte pas renonciation aux droits moraux (a. 14.1(3) L.D.A.). Le titulaire ne peut donc plus exercer ce droit, désormais propriété du nouveau titulaire-cessionnaire. La licence de droit d'auteur: le titulaire du droit d'auteur conserve la propriété du droit économique concerné, mais il autorise une tierce partie à exercer ce droit, et ce, selon des modalités établies à la licence. Il y a alors, selon la Loi, "concession d'un intérêt" dans le droit d'auteur concerné (a. 13(4) L.D.A.)* [171].

---

[167] *CCH Canadian Limited v. Law Society of Upper Canada*, [2004] 1 S.C.R. 339.
[168] Copyright Act, RSC 1985, c C-42, section 3.
[169] *Ibid.*, section 14.1. Section 28.2 specifies that the right to integrity is infringed only if the work (or its use in relation to a product, a cause, etc.) is modified in a manner prejudicial to the honour or reputation of the author; but in the same section we read "*In the case of a painting, sculpture or engraving, the prejudice referred to in subsection (1) shall be deemed to have occurred as a result of any distortion, mutilation or other modification of the work.*"
[170] *Ibid.*, section 13(4).
[171] BARIBEAU Marc, Principes généraux de la Loi sur le droit d'auteur, Édition 2007, Les publications du Québec, 2007, p. 75

Now that the general framework for granting the copyright, its scope and licences is defined, let us see how cloud computing companies manage copyright issues in their contracts.

The "additional clauses" of *Google Documents* specify in section 11.1:

> *You retain ownership of any intellectual property rights that you hold in that content. In short, what belongs to you stays yours. When you upload or otherwise submit content to our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content. The rights you grant in this license are for the limited purpose of operating, promoting, and improving our Services, and to develop new ones*[172].

Zoho, whose cloud computing service is essentially identical to that of *Google Documents*, includes in its contracts a clause to the same effect, but specifying that "*Unless specifically permitted by you, your use of the Services does not grant Zoho the license to use, reproduce, adapt, modify, publish or distribute the content created by you or stored in your user account for Zoho's commercial, marketing or any similar purpose*[173]."

Microsoft's contract also contains an almost identical clause: "*we don't claim ownership of the content you provide on the service. Your content remains your content. (…) You understand that Microsoft may need, and you hereby grant Microsoft the right, to use, modify, adapt, reproduce, distribute, and display content posted on the service solely to the extent necessary to provide the service*[174]."

The *MobileMe* contract calls things by their name and clearly mentions the service contract that the user grants the company simply by using the service:

> *Except for material we may license to you, Apple does not claim ownership of the materials and/or Content you submit or make available on the Service. However, by submitting or posting such Content on areas of the Service that are accessible by the public, you grant Apple a worldwide, royalty-free, non-exclusive license to use, distribute, reproduce, modify, adapt, publish, translate, publicly perform and publicly display such Content on the Service solely for the purpose for which such Content was submitted or made available. Said license will terminate within a commercially reasonable time after you or Apple remove such Content from the public area. By submitting or posting such Content on areas of the Service that are accessible by the public, you are representing that you are the owner of such material and/or have authorization to distribute it*[175].

According to the formulation of those licences, they are granted to companies, through those contracts, only to provide the service ("*solely to the extent necessary to provide the service"* or "*solely for the purpose for which such Content was submitted or made available*"). It remains to

[172] Google Documents, Terms [Online] http://www.google.com/google-d-s/intl/en/terms.html (page consulted on May 20, 2011).
[173] Zoho, Terms of Service [Online] http://www.zoho.com/terms.html (page consulted on May 17, 2011).
[174] Microsoft Service Agreement, [Online] http://explore.live.com/microsoft-service-agreement?ref=none (page consulted on May 17, 2011).
[175] MobileMe, Terms of Service, section 7 [Online] http://www.apple.com/legal/mobileme/en/terms.html (page consulted on May 17, 2011)

understand exactly what the scope of that licence is. The terms and formulation used are certainly broad enough to be left to interpretation.

Dropbox also does not claim ownership of material stored by means of this service. But the contract states that certain types of storage constitute licencing, but in favour of other users, not of the company:

> ***Votre dossier public***
> *While you own the content contained in Your Files, files placed in your public folders are automatically available to other Dropbox users and to the general public. By placing Your Files in your public folder, you hereby grant all other Dropbox users and the public a non-exclusive, non-commercial, worldwide, royalty-free, sublicensable, perpetual and irrevocable right and license to use and exploit Your Files in your public folder. In other words, a file in your public folder can be used by anyone, for any purpose* except *commercial use. If you do not want other people to be able to use Your Files in this manner, then simply do not place Your Files in your public folder. By placing Your Files in your public folder, you agree and acknowledge that Dropbox has no responsibility or obligation to monitor or notify of you of any non-compliance related to the license you have granted and that Dropbox has no responsibility to enforce or police, or aid you in enforcing or policing, the terms of that license.*
>
> ***Votre dossier partagé***
> *Tandis que vous êtes propriétaire du contenu de vos fichiers, les fichiers placés dans vos dossiers partagés deviennent accessibles aux utilisateurs auxquels vous aurez accordé un droit d'accès. En plaçant vos fichiers dans votre dossier partagé, vous acceptez et reconnaissez le fait que Dropbox n'a ni le devoir ni l'obligation de surveiller l'usage de vos fichiers ou de vous informer d'une quelconque violation relative aux droits ou aux licences que vous pouvez accorder à d'autres utilisateurs qui ont accès, le cas échéant, à vos dossiers partagés, et également que Dropbox n'est pas tenu d'appliquer ni de veiller à l'application des termes de ladite (lesdites) licence(s) ou autorisation(s) que vous avez accordée(s), ou de vous aider à le faire*[176].

Facebook's contract is less explicit as to the licence's finality, even though the contract mentions that content belongs to users; *Facebook* also grants the possibility of sub-licencing content protected by intellectual property rights:

> *For content that is covered by intellectual property rights, like photos and videos (IP content), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it*[177].

Yahoo!'s contract is the most detailed regarding licences granted, and specifies that the licences vary according to the content for which they are granted:

> *Yahoo! does not claim ownership of Content you submit or make available for inclusion on the Service. However, with respect to Content you submit or make available for inclusion on publicly accessible areas of the Service, you grant Yahoo! the following world-wide, royalty free and non-exclusive license(s), as applicable.*

[176] Dropbox, Terms of Service [Online] http://www.dropbox.com/terms (page consulted on May 17, 2011)
[177] Statement of Rights and Responsibilities, section 2.1, [Online] http://www.facebook.com/terms.php?ref=pf (page consulted on May 17, 2011)

- *With respect to Content you submit or make available for inclusion on publicly accessible areas of Yahoo! Groups, the license to use, distribute, reproduce, modify, adapt, publicly perform, and publicly display such Content on the Service solely for the purposes of providing and promoting the specific Yahoo! Group to which such Content was submitted or made available. This licence exists only for as long as you elect to continue to include such Content on the Service and will terminate at the time you remove or Yahoo! removes such Content from the Service.*
- *With respect to photos, graphics, audio, or video you submit or make available for inclusion on publicly accessible areas of the Service other than Yahoo! Groups, the license to use, distribute, reproduce, modify, adapt, publicly perform and publicly display such Content on the Service solely for the purpose for which such Content was submitted or made available. This licence exists only for as long as you elect to continue to include such Content on the Service and will terminate at the time you remove or Yahoo! removes such Content from the Service.*
- *With respect to Content other than photos, graphics, audio or video you submit or make available for inclusion on publicly accessible areas of the Service other than Yahoo! Groups, the perpetual, irrevocable and fully sublicensable license to use, distribute, reproduce, modify, adapt, publish, translate, publicly perform and publicly display such Content (in whole or in part) and to incorporate such Content into other works in any format or medium now known or later developed.*

The last point of the contract clause is the most problematic one. Indeed, the licence granted under the contract is perpetual and irrevocable (as in the *Dropbox* contract*)*. However, a perpetual contract cannot exist in Quebec; the longest term found in the Civil Code of Québec is that of emphyteutic contracts, which cannot have a term exceeding 100 years[178].

Under the common law, no prohibition is equally formal as to the term of a contract, but licencing contracts are revocable[179]. But under certain circumstances and when the laws allow it (which is the case only in certain specific economic sectors), judges have reassessed the clauses of some of those "perpetual" contracts, particularly when economic interests were at stake[180].

Some authors estimate that consumers could likely have the clause of an adhesion or consumer contract declared abusive if it provides "*une cession totale du droit d'auteur par le consommateur ou l'adhérent*[181]*.*" On that basis, we think it possible to invoke the abusive nature of licences as described in Yahoo! and Dropbox contracts – licences that resemble an assignment rather than an actual licence, given their formulation and scope.

Another peculiarity of this *Yahoo!* contract should be noted: the company is the only one to provide (again in section 8) the user's waiver of his moral rights – a waiver that is authorized (as

[178] For example, Civil Code of Québec, section 1880: "*The term of a lease may not exceed 100 years*.(…)" See also sections 1123, 1197 and 2376 of the Civil Code of Québec.
[179] "the pattern of the cases, of which Hillis Oil is a prominent example, is to regard all contracts as generally terminable on reasonable notice and to reject the view expressed by Lord Selborne that, apart from cases where some element of reliance, trust or confidence may exist, contracts lacking a termination provision are perpetual." SWAN Angela, Canadian Contract Law, Second Edition, Lexis Nexis, Markham 2009, p. 630.
[180] See: Cumberland Trust v. Maritime Electric (2000), 188 Nfld. & P.E.I.R. 178.
[181] BARIBEAU Marc, Principes généraux de la Loi sur le droit d'auteur, Édition 2007, Les publications du Québec, 2007, p. 78.

opposed to assignment) in section 14.1(2) of the Copyright Act: "*Moral rights may not be assigned but may be waived in whole or in part.*"

Marc Baribeau specifies what a licence or an assignment should contain to avoid any misunderstanding of its limits:

> *il semble préférable de confirmer par écrit les modalités de l'autorisation octroyée par le titulaire ; le contenu de cet écrit devrait préciser l'œuvre concernée et l'étendue des droits cédés ou autorisés : 1° quels droits sont visés : reproduction, publication, traduction, adaptation, etc. ; 2° les fins visées par l'autorisation ou la cession (à quel usage précis l'autorisation est accordée au tiers) ; 3° le territoire pour lequel la licence est octroyée ou la cession est accordée ; 4° dans le cas d'une licence : est-elle transférable à quelqu'un d'autre ou non?; celle-ci est-elle exclusive ou non?; 5° la durée de la licence ou, le cas échéant, de la cession ; 6° une compensation financière est-elle exigée (montant forfaitaire, redevances, etc.) pour cette licence ou cession, notamment lorsque cette disposition est accessoire à un contrat principal?; 7° les garanties accordées par le titulaire au licencié ou cessionnaire*[182].

Some of the licences mentioned do not contain all those elements, which can be a source of uncertainty and thus subject to disputes regarding unauthorized uses by means of the licence. But the Act provides mandatory content requirement for the licences, which do not even have to be written (except for exclusive licences)[183]. However, all cloud computing services (and all contents that may be posted there by users) will not face copyright claims, unless the company uses those documents for commercial purposes without having obtained the right to do so. In fact, the consumer generally does not care to grant copyright licences if he places such documents in private storage areas.

On the other hand, services such as Facebook that enable users to share content are more likely to face copyright claims from users, and should thus have very detailed copyright licences. Does sharing content mean that users do not attach much importance to such licences and will not claim their copyright royalties for those creations? Here again, if those contents are commercially exploited, consumers will doubtless want to recover their rightful share of revenues.

In short, the only incongruities raised with regard to the Copyright Act are related to licences that would be excessive, even abusive, by being irrevocable or perpetual.

[182] *Ibid.*

[183] Robertson v. Thomson Corp., 2006 SCC 43, paragraph 56: "We are satisfied that Weiler J.A. was correct in concluding that only an exclusive licence must be in writing. If Parliament intended for any type of non-exclusive licence to be deemed a "grant of an interest" requiring a written contract, it could have explicitly provided so just as it did for exclusive licences in s. 13(7)."

6.1 Possible Remedies

The Copyright Act provides that:

> *(1) Where copyright has been infringed, the owner of the copyright is, subject to this Act, entitled to all remedies by way of injunction, damages, accounts, delivery up and otherwise that are or may be conferred by law for the infringement of a right.*
>
> *(2) In any proceedings for an infringement of a moral right of an author, the court may grant to the author or to the person who holds the moral rights by virtue of subsection 14.2(2) or*
>
> *(3) As the case may be, all remedies by way of injunction, damages, accounts, delivery up and otherwise that are or may be conferred by law for the infringement of a right.*

Small claims courts are competent to hear Copyright claims. But except when a work is commercially exploited to the detriment of the author or in violation of the licence, or when it causes substantial economic loss to the user, consumers are not inclined to sue those companies for infringing the Copyright Act, as they often do in consumer affairs, because the various obstacles (time and all manner of costs) outweigh the modest economic gain at stake.

Concerning moral rights, we may assume that a remedy would be economically profitable only in situations when authors are famous, or when harm to the work's integrity and the prejudice incurred are so substantial as to warrant sufficient compensation to the author.

7 Cloud Computing Contracts in the Light of Privacy Acts

In Canada, the purpose of the Personal Information Protection and Electronic Documents Act[184] (hereinafter PIPEDA) is:

> *[…] to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances*[185]*.*

The Act thus has a double purpose, and rests on a balance between the two needs it is intended to meet – the circulation and exchange of information, and the protection of the right of privacy.

As we have seen, cloud computing companies require users to provide their personal information; this is their consideration, the price they pay for the monetarily free service. However, the companies are no less subject to obligations regarding this collection and use of users' personal information.

Our study will focus on the framework provided by PIPEDA, rather than on provincial laws to the same effect. In some Canadian provinces (Quebec[186], Alberta[187] and British Columbia[188]), there are laws recognized as essentially similar to PIPEDA and applicable rather than PIPEDA in those provinces, regarding the collection, use or communication of personal information that take place within the province. But PIPEDA takes precedence when the collection, use or communication of personal information takes place outside the province or when personal information is transferred, for example, from one province to another, or abroad. The cloud computing services currently on the market are mainly American, and the servers are located across the globe – we have selected for our study no Canadian cloud computing service that acts exclusively within a province.

PIPEDA applies to "*every organization in respect of personal information that the organization collects, uses or discloses in the course of commercial activities*," i.e., "*any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists*[189]*.*"

As mentioned in a preceding section (Cloud Computing Contracts: Consumer Contracts), we think it evident that the cloud computing companies we studied are commercial enterprises. The fact that those companies are financed by advertising based precisely on their collection of the

[184] Personal Information Protection and Electronic Documents Act (S.C. 2000, ch. 5).
[185] *Ibid.*, section 3.
[186] Act respecting the protection of personal information in the private sector, R.S.Q., chapter P-39.1.
[187] Personal Information Protection Act, S.A. 2003, c. P. 6-5.
[188] *Ibid.*, S.B.C. 2003, c. 63.
[189] Act respecting the protection of personal information in the private sector, R.S.Q., chapter P-39.1, section 4(1).

personal information of the users of their services confirms that this characterization also belongs to PIPEDA's sphere of application. The decision of the Privacy Commissioner of Canada following his investigation of the Facebook service confirms the soundness of this conclusion that those companies are subject to the provisions of PIPEDA: "*Facebook uses such personal information in the course of commercial activities*[190]."

To know how PIPEDA applies to foreign companies with which Canadian consumers do business online, it is necessary to read the decision of the Federal Court in the *Lawson v. Accusearch* case. The website *Abika.com* belonging to the company *Accusearch* proposed "*search services on individuals including background checks, psychological profiles, e-mail traces, unlisted and cell phone numbers, automobile licence plate details and criminal records.*"[191] In fact, the company collected and used personal information about Canadians, although the company had its head office and principal place of business in the United States. A Canadian citizen had complained before the Office of the Privacy Commissioner of Canada against *Accusearch*; however, the Privacy Commissioner of Canada had refused to investigate the complaint, while estimating that the citizen was not competent to investigate the American company.

The Federal Court reversed the decision of the Privacy Commissioner of Canada. In subsections 38 and following of its decision, the Court stated that:

> *[Parliament cannot have intended that PIPEDA govern the collection and use of personal information worldwide. For instance, if Ms. Lawson were an American working in the United States, PIPEDA would have no application. Regulatory and investigative functions (as opposed to judicial) must have some connection with the state which enacts the underlying legislation. However, I believe the Privacy Commissioner erred in law by taking the position that Ms. Lawson's complaint could only be investigated if Parliament had intended and had given extraterritorial effect to PIPEDA. (…)It would be most regrettable indeed if Parliament gave the Commissioner jurisdiction to investigate foreigners who have Canadian sources of information only if those organizations voluntarily name names. Furthermore, even if an order against a non-resident might be ineffective, the Commissioner could target the Canadian sources of information. I conclude as a matter of statutory interpretation that the Commissioner had jurisdiction to investigate, and that such an investigation was not contingent upon Parliament having legislated extraterritorially as permitted by the* Statute of Westminster, 1931*[(U.K.), 22 Geo. V, c. 4 [R.S.C., 1985, Appendix II, No. 27]]*[192].

In short, "*PIPEDA* [Personal Information Protection and Electronic Documents Act] *does give the Privacy Commissioner jurisdiction to investigate complaints relating to the trans-border flow of personal information*[193]."

---

[190] PIPEDA Case Summary #2009-008 Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. under the Personal Information Protection and Electronic Documents Act, by Elizabeth Denham, Assistant Privacy Commissioner of Canada.[Online] http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.asp (page consulted on May 20, 2011). In the *Letter from OPC to CIPPIC outlining its resolution with Facebook*, dated August 25, 2009, the Commissioner provides information on founded allegations, outstanding recommendations, and Facebook's commitments regarding certain issues considered founded and resolved. [Online] http://www.priv.gc.ca/media/nr-c/2009/let_090827_e.asp (page consulted on January 16, 2012).

[191] Lawson v. Accusearch Inc. (c.o.b. abika.com), 2007 CF 125.

[192] *Ibid.*

[193] KNIGHT Jamie, Sharon CHILCOTT and Melanie McNaught, Canada Personal Information Protection and Electronic Documents Act Quick reference 2010 Edition, Toronto, Carswell, 2010, p.29 and foll.

The Personal Information Protection and Electronic Documents Act is based on 10 principles, stated in Schedule I of the Act, that are modelled on the OECD Council recommendation for Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[194]. The principles are: 4.1) accountability, 4.2) identifying purposes, 4.3) consent, 4.4) limiting collection, 4.5) limiting use, disclosure and retention of personal information, 4.6) accuracy, 4.7) safeguards, 4.8) openness, 4.9) individual access, 4.10) challenging compliance.

Our study will analyse cloud computing contracts in the light of some of these principles, i.e., those we think most likely to raise problems. The principles are those of accountability (4.1), de consent (4.3), safeguards (4.7) and openness (4.8).

7.1 Analysis of Cloud Computing Contracts in the Light of the Principle of Openness

4.8 Principle 8 — Openness

> *An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information*[195]*.*

Section 4.8.1 adds: "*This information shall be made available in a form that is generally understandable.*"

This principle imposes to companies that collect and use personal information an obligation to provide information about their practices in matters of personal information management. Information addressed to users of cloud computing services must be accurate, accessible and understandable.

Cynthia Chassigneux perfectly summarizes how this obligation to inform binds companies: "*La transparence des entreprises en ligne doit conduire les gestionnaires de sites marchands à tout mettre en œuvre pour permettre aux internautes de prendre connaissance des engagements contenus dans les politiques de confidentialité*[196]*.*"

This principle is strongly related to the principle of consent, which we will examine below – indeed, there can be no free and informed consent to a collection of information without open information on what such a transmission of information implies.

Following a complaint by the Canadian Internet Policy and Public Interest Clinic (CIPPIC), the Privacy Commissioner investigated *Facebook*'s practices in 2008. The investigation mainly attempted to know whether "*Facebook was providing a sufficient knowledge basis for meaningful consent by documenting purposes for collecting, using, or disclosing personal*

[194] OECD Council recommendation for Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, [Online] http://www.oecd.org/document/18/0,3746,en_2649_34223_1815186_1_1_1_1,00.html (page consulted on May 20, 2011).
[195] Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, Principle 8.
[196] CHASSIGNEUX Cynthia, Vie privée et commerce électronique, Éditions Thémis, Montreal, 2004, p. 189.

information and bringing such purposes to individuals' attention in a reasonably direct and transparent way[197]*.*"

Regarding the principle of openness, it should be noted that the Assistant Privacy Commissioner mentions, regarding *Facebook*'s practices:

> *Firstly, in consideration of Principles 4.1.4(d), 4.2.1, 4.3.2, and 4.8, I am concerned that, given the prominent and essential role that advertising plays in its business, Facebook is not making a reasonable enough effort to document and explain in its Privacy Policy its use of advertising, its use of users' information for purposes of targeted advertising, and the extent of users' ability to opt out of Social Ads*[198]*.*

The Assistant Commissioner's conclusion on *Facebook's* practices is unequivocal: "*In sum, in respect of documenting and explaining purposes related to advertising, I find that Facebook has failed to meet a reasonable standard in the circumstances, as envisaged by Principles 4.1.4(d), 4.2.1, 4.3.2, and 4.8*[199]*.*"

On the basis of what we have observed in studying the policies of the various cloud computing companies we have examined, we may easily conclude that other companies could well be concerned by the investigations of the Privacy Commissioner of Canada. Indeed, many of the policies we have analysed are far from complying with the transparency principle imposed by PIPEDA; information given to users through privacy policies are too often incomplete.

For example, *Apple*'s commitment to confidentiality regarding its *MobileMe* service mentions notably that "*At times Apple may make certain personal information available to strategic partners that work with Apple to provide products and services, or that help Apple market to customers*[200]*."* What personal information will be made available to strategic partners? What does "*at times*" mean, in terms of frequency? How will the disclosed information be used by *Apple*'s partners? Etc.

We also find in the "*Microsoft Online Privacy Statement*" a clause that announces some of the uses that will be made of the personal information collected: in particular, cross-references with information obtained from other *Microsoft* services *or from other companies*, not identified, and for very vague purposes: "*In order to offer you a more consistent and personalized experience in your interactions with Microsoft, information collected through one Microsoft service may be combined with information obtained through other Microsoft services. We may also supplement the information we collect with information obtained from other companies* [201]*.*"

---

[197] PIPEDA case summary #2009-008 – Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. under the *Personal Information Protection and Electronic Documents Act*, by Elizabeth Denham, Assistant Privacy Commissioner of Canada. [Online] http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.asp (page consulted on May 20, 2011).
[198] *Ibid.,* paragraph 136.
[199] *Ibid*., paragraph 138.
[200] MobileMe Privacy Policy, [Online] http://www.apple.com/privacy/ (page consulted on May 20, 2011).
[201] Microsoft Online Privacy Statement, [Online] http://privacy.microsoft.com/en-ca/fullnotice.mspx (page consulted on May 20, 2011).

This type of clause can certainly not be considered limpid for users. While a will to inform users is expressed, the result leaves much to be desired: in the end, users are not actually better informed about certain issues that appear essential.

Google has a similar confidentiality clause, with the same shortcomings: "*We may combine personal information from one service with information, including personal information, from other Google services – for example to make it easier to share things with people you know*[202]."

However, the "*Microsoft Online Privacy*" declaration is extremely detailed: over 6 pages of information containing essential points. For instance, we learn that the consumer may refuse to have his personal information used in order to target advertisements to him. But it would be surprising if users of *Microsoft*'s cloud computing services actually read such a long policy statement. Does such a text meet the accessibility requirements? Can we consider that Microsoft is providing information "*in a form that is generally understandable*?"

The clause contained in the user contract of *Norton Online Backup* is as clear as it is brief. Section 9 of the contract provides the type of data that may be collected by *Symantec* and their specific use for the service's features; but there is a vaguer mention about what the company may collect (*"certain anonymous security information"*) and share for purposes of detecting and preventing Internet security risks[203].

7.2 Analysis of Cloud Computing Contracts in the Light of the Principle of consent

4.3 Principle 3 — Consent

Consent is the cornerstone of policies for collecting and using personal information. This can be noted in reading section 4.3.1, Schedule I of the Personal Information Protection and Electronic Documents Act:

> *Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified)*[204].

The Federal Court of Appeal reached a similar conclusion in the *Wansink v. Telus Communications Inc.* decision, in which Judge Décary writes:

> *Consent to collection of personal information is so much a cornerstone of the Act that subsections 2(2) and 7(1) expressly require that the note to clause 4.3 be disregarded when interpreting a reference to that clause. Considering that the note to clause 4.3 states that "In certain*

[202] Privacy Centre, Privacy Policy [Online] http://www.google.com/intl/en/policies/privacy/ (page consulted on May 20, 2011).
[203] Norton Online Backup. Terms of service agreement. [Online] http://www.symantec.com/content/en/us/about/media/NOBU_TOS_21_USE.pdf (page consulted on January 16, 2012).
[204] PIPEDA, Schedule I, section 4.3.1.

> *circumstances personal information can be collected…without the knowledge and consent of the individual," the very fact that Parliament has expressly asked that the note be ignored is a significant indication of its desire to limit the circumstances in which consent to collection of personal information is not required to those it describes in subsection 7(1)*[205].

In fact, there is a general rule, which applies to all companies in all cases with regard to any personal information: the latter cannot be collected or used without the consent of the person concerned. The rare circumstances stated in section 7 of the Act present exceptional cases where personal information may be collected or used without prior consent.

As mentioned above, the principle of consent is closely related to that of openness. Section 4.3.2, Schedule I of PIPEDA specifies:

> *The principle requires "knowledge and consent". Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.*

To be valid, consent must be manifest, free and informed. In other words, the consumer's consent must be evident and undeniable, in addition to having been obtained without coercion and given knowingly[206].

As indicated in section 4.3.7, Schedule I of PIPEDA, "*Individuals can give consent in many ways.*" In this regard, the Privacy Commissioner of Canada has already mentioned:

> *that he regards and promotes positive or "opt-in" consent as the most appropriate and respectful form for organizations to use in any circumstances. Nevertheless, in deference to Principle 4.3.4, he recognized that the negative or "opt-out" form was acceptable in some strictly defined circumstances - notably, where the personal information is demonstrably non-sensitive, where the consent-seeking process meets the individual's reasonable expectations under Principle 4.3.5, and where the organization is otherwise in compliance with all relevant provisions of the Act*[207].

According to the Office of the Privacy Commissioner of Canada, positive or "opt-in" (express) consent takes place when "*the organization presents an opportunity for the individual to express positive agreement to a stated purpose*[208]*."* Negative or "opt-out" consent enables the organization to offer "*the individual with an opportunity to express non-agreement to an identified purpose. Unless the individual takes action to "opt out" of the purpose — that is, say "no" to it — the organization assumes consent and proceeds with the purpose*[209]."

According to the Privacy Commissioner, negative (or "opt-out") consent is acceptable only under the following conditions: the information must not be sensitive; disclosure of the information

[205] *Wansink v. Telus Communications Inc.*, 2007 CAF 21 in subsection 21.
[206] CHASSIGNEUX Cynthia, Vie privée et commerce électronique, Éditions Thémis, Montreal, 2004, pp. 147 and 150.
[207] Commissioner's findings – PIPEDA Case Summary #2003-207: Cellphone company meets conditions for "opt-out" consent, [Online] http://www.priv.gc.ca/cf-dc/2003/cf-dc_030806_02_e.asp (page consulted on May 20, 2011).
[208] Office of the Privacy Commissioner of Canada, Fact Sheets: Determining the appropriate form of consent under the Personal Information Protection and Electronic Documents Act, [Online] http://www.priv.gc.ca/resource/fs-fi/02_05_d_24_e.asp (page consulted on May 30, 2011).
[209] *Ibid.*

must be limited and well defined; and the company's intentions must be circumscribed, well defined and stated in a reasonably clear and understandable manner to the individual when his personal information is collected. A company that collects and uses personal information on the basis of negative consent must put in place an efficient, easy and low-cost procedure enabling users to terminate the agreement or withdraw their consent in case of secondary use of personal information for marketing purposes[210].

Finally, the importance of those provisions with regard to consent when they are applied to the Internet is perfectly summarized by Cynthia Chassigneux:

> *(…) cette prise en considération du consentement préalable et explicite à la collecte s'explique par le fait que sur Internet, il est important que la personne concernée exprime réellement sa volonté d'accepter ou non que ses données personnelles soient collectées. Cette idée vise à protéger la partie la plus faible au contrat, c'est-à-dire l'internaute*[211].

It is not surprising to find the negative consent procedure in some cloud computing contracts when they announce the use of personal information for advertising purposes. Colin McNairn explains this secondary use for marketing purposes:

> *Secondary marketing involves the solicitation of a Customer, on the basis of personal information, for the sale of goods or services other than those in connection with which that information was collected or generated. The marketing may be conducted by the organization that originally collected or generated the personal information, one of its affiliates or some persona at arm's length to which the organization has passed on the information or which it has facilitated targeted marketing with the benefit of the information. The use of the information for such marketing is secondary to the purpose for which it was originally collected or generated*[212].

Indeed, in cloud computing contracts, a distinction should be drawn between the consumer's consent to the company's collection of personal information in order to operate the service, and the consent he should be able to express to the company's use of personal information for secondary purposes of targeted advertising – a purpose for which companies preferably use negative consent. But in some cases it is difficult for the consumer to express his objection to the use of personal information for secondary purposes, because companies "conceal" information on this possibility of withdrawing his consent.

We find in *Microsoft*'s contract the use of negative consent to secondary uses for advertising purposes. But the company cannot be reproached for a lack of transparency: the clause pertaining to advertisements is extremely detailed. However, only at the end of the clause is it mentioned that consumers may refuse that their personal information be used for purposes of targeted advertising.

Does *Microsoft*'s use of negative consent meet the conditions set by the Privacy commissioner? The information collected does not seem particularly sensitive: it does not concern the health of

[210] Commissioner's findings – PIPEDA Case Summary #2003-207: Cellphone company meets conditions for "opt-out" consent, [Online] http://www.priv.gc.ca/cf-dc/2003/cf-dc_030806_02_e.asp (page consulted on May 20, 2011).
[211] CHASSIGNEUX Cynthia, Vie privée et commerce électronique, Éditions Thémis, Montreal, 2004, p.154.
[212] McNAIRN Colin H.H., A Guide to the Personal Information Protection and Electronic Documents Act, LexisNexis, Markham, 2010, p. 60.

users or financial information. As for the nature of the personal information that will be used, this is formulated in an extremely broad manner:

> *demographic or interest data, including any you may have provided when creating an account (e.g. age, zip or postal code, gender), demographic or interest data acquired from other companies and a general geographic location derived from your IP address, (b) the pages you view and links you click when using Microsoft's and its advertising partners' websites and services, (c) the search terms you enter when using Microsoft's Internet search services, such as Bing, and (d) information about the users you most frequently interact with through Microsoft's communications or social networking services, such as Messenger. For more information about how we target ads, visit Personalized Advertising from Microsoft* [213].

In short *Microsoft* announces that all data collected will be used. Disclosure of this information is neither limited nor well defined.

There is no doubt that the company intends to have a very detailed profile of users to provide them with targeted advertising (or have it provided to them, since advertising is purchased from *Microsoft* by advertisers wanting to reach a target clientele). But it does not suffice that those intentions can be guessed: they must be stated in a reasonably clear and understandable manner to be indicated to the person when his personal information is collected.

All major companies use negative consent regarding compromising advertising. For example, a page on *Yahoo!*'s website is dedicated to "opt-out" consent. As the company mentions, "*We use information about many of the pages you have visited, ads you have seen and clicked, and some of your searches on Yahoo! to create interest categories that help us choose the kinds of ads you'll see. You can edit or de-select categories here or opt out of interest-based ads altogether*." This clause appears to state that the company nevertheless limits the information what will be used for targeted advertising purposes. But there is very little information to enable informed consent.

Similarly, in its confidentiality rules, *Google* adds links to targeted advertising; one must navigate from page to page on the Google website to finally arrive at a page enabling the user to deactivate the feature allowing the company to send targeted advertising.

Consent, whether positive ("opt-in" — the company requests consent before collecting and using information) or negative ("opt-out" — the company assumes consent until the consumer notifies it to the contrary), pertains in all cases to the collection and use of users' personal information. If the consumer chooses (after discovering that it is possible) to withdraw his consent, the company should, according to the law, cease all collection and use of his personal information for the purposes he has refused. Thus, if the company uses negative consent regarding the use of personal information for targeted advertising purposes, it is vaguely worrisome that the option offered to the consumer is not to prevent the collection and use of his information for that purpose, but only to stop receiving targeted advertising (*Yahoo!*: "*opt out of interest-based ads*", *Microsoft:* "*If you don't want to see personalized ads from Microsoft, you can choose not to receive these types of ads*[214]").

[213] Microsoft Online Privacy Statement, [Online] http://privacy.microsoft.com/en-ca/fullnotice.mspx (page consulted on May 20, 2011).
[214] Microsoft Advertising. Personal Advertising from Microsoft, [Online] http://choice.live.com/advertisementchoice/ (page consulted on June 27, 2011).

This complex navigation (coupled with a negative consent practice) contradicts the principle of transparent information enabling informed consent. The Privacy Commissioner of Canada has already indicated the necessary elements for obtaining such informed consent in the case of an "opt-out." Collin McNair summarizes them as follows:

> *First, any potential use or disclosure of personal information for secondary marketing purposes must be made known to the consumer at the time he or she has the opportunity to opt out. It is not enough that it is evident from the institution's privacy Policy if a copy of that Policy is not supplied to the consumer at the relevant time. Second, notice of the potential use or disclosure, if printed, must not be in such small print or be so legalistic as to be difficult to read or understand. Third, any notice that is very broad in its terms may not be sufficiently informative*[215]*.*

We quoted above a survey indicating that 68% of users of at least one cloud computing application said they were concerned by the fact that the company providing them with the services can analyse their personal information and then send them targeted advertising. This result implies that consumers are not aware of the number of companies that actually analyse data in view of targeting advertisements. Section 4.3.2, Schedule I of PIPEDA nevertheless states that "*Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed*."

[215] McNAIRN Colin H.H., A Guide to the Personal Information Protection and Electronic Documents Act, LexisNexis, Markham, 2010, p. 61.

7.3 Analysis of Cloud Computing Contracts in the Light of the Principle of Safeguards

4.7 Principle 7 — Safeguards

The principle of safeguards provides that "*Personal information shall be protected by security safeguards appropriate to the sensitivity of the information*[216]."

Accordingly, certain obligations are imposed on the companies: the latter must take adequate security measures to protect personal information, particularly against theft or loss[217]. To be adequate, the safety of personal information must be suited to the sensitivity of personal information – personal health information or financial information will require greater safeguards.

From users' viewpoint, there is a certain subjectivity in security expectations, which may vary according to the type of service used. For example, using a social networking website implies that some data will be disclosed to other users of the website. Given that such data are part of those collected by the company that provides the social networking service, the user still expects the information he has chosen not to disclose publicly will not be disclosed due to a breach of security, for example. As we have seen, some services are not free of charge, and users of those services expect that the financial information they have consented to providing will not be disclosed to other users (or to anyone who may have access to the website). Similarly, if someone uses a data storage service, he expects that what he stores on the website, including everything that may be considered personal information, is secure and that the data will not be disclosed to or accessible by other users.

How can one know whether personal information stored by cloud computing services is well protected by the companies, and whether the latter establish safeguards suitable for the level of sensitivity of such personal information?

Unless a violation of confidentiality reveals inadequate safeguards, consumers will very rarely be able to know companies' safeguards. This occurred lately with Sony's online PSN gaming website, which was attacked by hackers who obtained the personal information of over 20 million people. The reactions were swift: the users launched lawsuits in the United States[218] and Canada[219], and the company is being investigated by American, British, Irish, Australian and Italian privacy protection authorities[220]. Those investigations will reveal precisely the level of security that was applied by the company and to judge whether it was sufficient.

---

[216] Act respecting the protection of personal information in the private sector, R.S.Q., chapter P-39.1, Annex I, section 4.7.
[217] *Ibid.,* Annex I, section 4.7.1.
[218] McELROY Griffin, Class action lawsuit filed against Sony for security breach, Joystiq, April 27, 2011 [Online] http://www.joystiq.com/2011/04/27/class-action-lawsuit-filed-against-sony-for-security-breach/ (page consulted on May 20, 2011).
[219] RANSOM-WILEY James, Canadian firm proposes class action against Sony to the tune of $1B in damages, Joystiq Network website, United States, May 4, 2011. http://www.joystiq.com/2011/05/04/canadian-firm-proposes-class-action-against-sony-to-the-tune-of/ (page consulted on May 20, 2011).
[220] Piratage du PSN : la facture pourrait être salée pour Sony, [Online] http://www.20minutes.fr/article/721359/piratage-psn-facture-pourrait-etre-salee-sony (page consulted on May 20, 2011).

The seventh principle imposes, on companies offering cloud computing services, an obligation to protect personal information by means of "*security safeguards appropriate to the sensitivity of the information.*" While this principle does not oblige companies to disclose the safeguards adopted, the eighth principle, that of openness, specifies that "*An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.*" (4.8). Among the information on policies and practices that the company must make available to users is a description of the means of access to the personal information kept by the organization, as well as the organization's standards or codes (4.8.2). On that basis, it appears reasonable to estimate that companies must make available to users information on the safeguards adopted. A user who stores personal information on a cloud computing service might reasonably want to choose, on the basis of the level of protection that the company is able to offer, which service he will accept to use.

However, a balance should be found between openness and security imperatives. The Privacy Commissioner of Canada has been interested in the subject after a consumer filed a complaint against a bank. The consumer, a victim of identity theft by an employee of his bank, demanded to obtain the bank's policies and practices regarding fraud. The Privacy Commissioner of Canada "*noted that this complaint raised the issue of how an organization strikes a balance between its obligations under the Act to inform the public about its policies and procedures to protect personal information in its care and to ensure the effectiveness of the safeguards it has in place to protect that information."* In this instance, the Commissioner was of the view "*that a bank must take a broader view of the consequences of making detailed information about its policies and procedures available. He found it logical that a bank would not want to publicize the specific steps it takes to prevent fraud because to do so would give criminals information about how to circumvent the bank's safeguards*[221]*.*"

So let us see what the companies indicate in their cloud computing contracts about the safeguards adopted to protect personal information.

Some companies limit disclosure to a declaration that reasonable measures are taken to protect the security of the personal information of the users of cloud computing services. This is the case, for example, with *Zumodrive* and *Dropbox*. The latter, which professes concern for the security of that information, simply states that it has adopted reasonable safeguards of its customers' personal information against any unauthorized access, and does not go into details[222].

The company that provides the *Zumodrive* service also mentions the establishment of reasonable measures to prevent unauthorized access, modifications, destruction or damage to personal information and other data entrusted to it, but does not detail what those measures are in the case of personal information. However, it details the safeguards it employs to protect the data it stores[223].

For its part, *Adrive* declares that it uses the best practices to protect its customers' personal information, but reveals none of those practices, except for those put in place to protect

[221] Commissioner's findings – PIPEDA Case Summary #2003-183: Bank not required to publicize detailed privacy policies and procedures [Online] http://www.priv.gc.ca/cf-dc/2003/cf-dc_030710_03_e.asp (page consulted on May 30, 2011)
[222] Dropbox Privacy, [Online] http://www.dropbox.com/privacy (page consulted on May 20, 2011).
[223] Zumodrive Privacy, [Online] http://www.zumodrive.com/privacy (page consulted on May 20, 2011).

sensitive data (such as credit card numbers), i.e., SSL encryption. *Adrive* adds that "*All of our Users' information is restricted in our offices*[224]."

Zoho also indicates that it applies industry standards for data security:

> *We adopt industry appropriate data collection, storage and processing practices and security measures, as well as physical security measures to protect against unauthorized access, alteration, disclosure or destruction of your Personal Information, username, password, transaction information and data stored in your user account*[225].

We observe a little more transparency in the case of *Microsoft*, which mentions that it uses:

> *(…) a variety of security technologies and procedures to help protect your personal information from unauthorized access, use, or disclosure. For example, we store the personal information we collect on computer systems with limited access, which are located in controlled facilities. When we transmit highly confidential information (such as a credit card number or password) over the Internet, we protect it through the use of encryption, such as the Secure Socket Layer (SSL) protocol* [226].

Apple, for its *MobileMe* service, gives the same information as in Microsoft's privacy policy[227].

Google and *Yahoo!* are the most transparent about the safeguards they use. The object is not to disclose all safeguards, but to attain a balance between the need to protect the safeguards themselves by not revealing them in detail, and the openness to which users are entitled from those companies. The simple fact of saying that the company uses reasonable safeguards, even if such is the case, may not comply with the principle of openness.

Google and *Yahoo!* Provide much more security information and thus appear to have attained a balance between the two principles.

Thus, *Google* specifies the following:

> *We work hard to protect Google and our users from unauthorized access to or unauthorized alteration, disclosure or destruction of information we hold. In particular: We encrypt many of our services using SSL; we offer you two step verification when you access your Google Account, and a Safe Browsing feature in Google Chrome; we review our information collection, storage and processing practices, including physical security measures, to guard against unauthorized access to systems; we restrict access to personal information to Google employees, contractors and agents who need to know that information in order to process it for us, and who are subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations*[228].

In addition, *Google* maintains a blog on the security of its services.

---

[224] Adrive Privacy Policy [Online] http://www.adrive.com/privacy (page consulted on May 20, 2011).
[225] Zoho Privacy [Online] http://www.zoho.com/privacy.html (page consulted on May 20, 2011).
[226] Microsoft Online Privacy Statement, [Online] http://privacy.microsoft.com/en-ca/fullnotice.mspx (page consulted on May 20, 2011).
[227] MobileMe Privacy Policy [Online] http://www.apple.com/privacy/ (page consulted on May 30, 2011).
[228] Google Privacy Policy, [Online] http://www.google.com/intl/en/policies/privacy/ (page consulted on May 20, 2011).

Yahoo! Gives the most information on the security of its various cloud computing services[229]. Indeed, on the Security page of the *Yahoo! Privacy Center* are listed some of the company's safeguards of personal information. Like the other companies, *Yahoo!* uses the "Secure Socket Layer" for the transmission of banking information during payable transactions. Moreover, a security key may be requested for certain *Yahoo!* Services. Measures are also taken to ensure the security of data storage. In addition, *Yahoo!* mentions that it trains its employees in personal information security.

Symantec's only mention of data protection regarding its *Norton Online Backup* service pertains to some of the information it collects to provide the service to the user: the data will be encrypted[230]. The service contract does not disclose anything about the security of the service itself.

7.4 Analysis of Cloud Computing Contracts in the Light of the Principle of Accountability

4.1 Principle 1 — Accountability

The principle of accountability is stated in section 4.1, Schedule I of PIPEDA as follows: "*An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.*"

Section 4.1.3 extends this principle of accountability by adding that

> *An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.*

Cloud computing companies that do business with a Canadian user remain accountable for the personal information provided by that user, even when they outsource certain services or store such information in servers located in other countries, which may be managed by third parties.

With regard to cloud computing services, companies may have personal information handled by other companies, which may well be located abroad: behavioural advertising services, data storage, etc. Those third party companies may have access to users' personal information. Under those circumstances, what are the responsibilities of a company that offers the cloud computing service and has collected and used the personal information of users?

First we note that all the cloud computing contracts we have examined contained a clause indicating that personal data would be transferred to the United States, and even, in the case of Apple and Symantec, in any country where the company does business.

[229] Security at Yahoo!, [Online] http://info.yahoo.com/privacy/us/yahoo/security/ (page consulted on May 20, 2011)
[230] Norton Online Backup. Terms of service agreement. [Online] http://www.symantec.com/content/en/us/about/media/NOBU_TOS_21_USE.pdf (page consulted on January 16, 2012).

In the privacy policy section on outsourcing (i.e., transferring data to a third party in order to operate the service, often through outsourcing), *Dropbox* mentions that the company does business with third parties that will have access to personal information only for the provision of services outsourced by *Dropbox*, "(*including but not limited to data storage, maintenance services, database management, web analytics, payment processing, and improvement of the Site's features) or to assist us in analyzing how our Site and service are used*[231]." But nothing indicates that those third party companies receiving personal information are bound, by contract or otherwise, to apply a level of protection comparable to that which *Dropbox* is required to apply to personal information.

Zoho's privacy policy clearly states:

> *We may need to disclose Personal Information to our affiliates, service providers and business partners solely for the purpose of providing Zoho Services to you. In such cases Zoho will also ensure that such affiliates, service providers and business partners comply with this Privacy Policy Statement and adopt appropriate confidentiality and security measures*[232].

Microsoft's privacy policy specifies, regarding the possibility of outsourcing services:

> *Microsoft occasionally hires other companies (vendor) to provide limited services on our behalf, such as handling the processing and delivery of mailings, providing customer support, hosting websites, processing transactions, or performing statistical analysis of our services. Those service providers will be permitted to obtain only the personal information they need to deliver the service. They are required to maintain the confidentiality of the information and are prohibited from using it for any other purpose than for delivering the service to Microsoft in accordance with Microsoft's instructions and policies* [233].

Apple has a clause similar to that of *Microsoft*:

> *Apple shares personal information with companies who provide services such as information processing, extending credit, fulfilling customer orders, delivering products to you, managing and enhancing customer data, providing customer service, assessing your interest in our products and services, and conducting customer research or satisfaction surveys. These companies are obligated to protect your information and may be located wherever Apple operates*[234].

After advising that data may be transferred to a country that does not necessarily have legislation that protects data as well as the area where the user resides, mentions that "*[Symantec] has taken steps so that the Data, if transferred, receives an adequate level of protection, including by using data transfer agreements where required*[235]." (Our emphasis)

We note that the formulations of those clauses do not indicate in any way that a comparable level of protection of personal information must be put in place by the third party company.

[231] Dropbox Privacy, [Online] http://www.dropbox.com/privacy (page consulted on May 20, 2011).
[232] Zoho Privacy, [Online] http://www.zoho.com/privacy.html (page consulted on May 20, 2011).
[233] Microsoft Online Privacy Statement, [Online] http://privacy.microsoft.com/en-ca/fullnotice.mspx (page consulted on May 20, 2011).
[234] MobileMe Privacy Policy, [Online] http://www.apple.com/privacy/ (page consulted on May 20, 2011).
[235] Norton Online Backup. Terms of service agreement, [Online] http://www.symantec.com/content/en/us/about/media/NOBU_TOS_21_USE.pdf (page consulted on January 16, 2012).

Microsoft's contractual clauses only mention the confidentiality requirement, and apple only mentions data protection. This is far from the specifics provided by Google, which announces full compliance with PIPEDA:

> *We provide personal information to our affiliates or other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures*[236].

Yahoo! also has a somewhat general clause on the outsourcing of services and the sharing of information; but the company refers to confidentiality contracts with third party companies: "*We provide the information to trusted partners who work on behalf of or with Yahoo! under confidentiality agreements. These companies may use your personal information to help Yahoo! communicate with you about offers from Yahoo! and our marketing partners. However, these companies do not have any independent right to share this information*[237]."

Nevertheless, so long as a complaint is not filed with the Privacy Commissioner, who can then examine contracts (or other measures) that would require third party companies to guarantee a level of protection comparable to that required of the outsourcers, we cannot be certain that the outsourcing meets PIPEDA requirements. Users must therefore blindly trust the companies' declarations.

To compensate for the lack of transparency entailed by outsourcing, some large companies, such as *Apple*, *Microsoft* and *Facebook*, have opted for certification by third party companies, as in the *TRUSTe* program. *Microsoft* thus indicates in its privacy policy that it

> *(…) has been awarded TRUSTe's Privacy Seal signifying that this privacy statement and our practices have been reviewed by TRUSTe for compliance with TRUSTe's program requirements including transparency, accountability and choice regarding the collection and use of your personal information. The TRUSTe program does not cover information that may be collected through downloadable software. TRUSTe's mission, as an independent third party, is to accelerate online trust among consumers and organizations globally through its leading privacy trustmark and innovative trust solutions*[238].

A similar mention is found in the privacy policies of the cloud computing services of *Facebook*[239] and *MobileMe*[240], which also contain means for contacting the company about issues or complaints.

TRUSTe offers several certification programs. *Apple* has chosen the program to have its privacy policy certified. *Facebook* has in addition decided to obtain certification of its policy on the international exchange of personal information.

Cynthia Chassigneux summarizes the mechanics of certification and its effects on consumers:

[236] Google Privacy Policy, [Online] http://www.google.com/intl/en/policies/privacy/ (page consulted on May 20, 2011).
[237] Yahoo Privacy Policy, [Online] http://info.yahoo.com/privacy/ca/yahoo/ (page consulted on May 20, 2011).
[238] Microsoft Online Privacy Statement, [Online] http://privacy.microsoft.com/en-ca/fullnotice.mspx (page consulted on May 20, 2011).
[239] Facebook Data Use Policy [Online] https://www.facebook.com/policy.php (page consulted on May 20, 2011).
[240] Apple Privacy Policy [Online] http://www.apple.com/privacy/ (page consulted on May 20, 2011).

> *En apposant le label de l'autorité de certification, l'entreprise en ligne adhère aux conditions émises par cette dernière. En effet, le commerçant électronique accepte, d'une part, que ses engagements en matière de protection des renseignements personnels ou que ses mécanismes de sécurité soient soumis à l'examen d'un tiers et, d'autre part, que l'accréditation qui lui est accordée puisse lui être retirée en cas de manquement. L'adhésion, même si elle est volontaire, est donc conditionnelle au respect des règles mises en place par l'autorité de certification. Ainsi, en devenant titulaire d'un label, une entreprise en ligne gagnera en crédibilité aux yeux des internautes. Crédibilité qui fait référence aux notions de relation durable ou encore de réputation permettant de définir la notion de confiance*[241].

Still, this certification does not mean that privacy policies meet the requirements of countries such as Canada, since the certification is conferred by American companies, which operate according to their own standards. For example, a certification that would involve the Office of the Privacy Commissioner of Canada would reassure Canadian consumers that the privacy policies of certified companies comply with Canadian laws.

It is thus important to ensure that companies comply with the principles of accountability and openness toward their Canadian users.

Indeed, users of cloud computing services should be reassured that although personal information is transferred abroad, such information will have the same level of protection as in Canada.

However, as we have seen, transparency was often lacking in the outsourcing of services, since consumers did not have all relevant information to be certain that their personal information will be protected adequately. Accordingly, consumers should be fully aware of the risks and consequences of using those services, and aware that their personal information will be transferred abroad. Knight, Chilcott and McNaught report a troubling incident to that effect:

> *There have been a number of notable recent privacy breaches involving foreign outsourcing arrangements. For instance, in 2003, a medical transcriber in Pakistan threatened to post patients' medical records online unless she was paid outstanding wages. In 2004, employees of an outsourcing company in Bangalore, India, threatened to release American medical records unless they received payment from the American company that had contracted out the work*[242].

[241] CHASSIGNEUX Cynthia, "La confiance, instrument de régulation des environnements électroniques," (2007) 37 R.D.U.S. p.441, p.468.
[242] KNIGHT Jamie, Sharon CHILCOTT and Melanie McNaught, Canada Personal information protection and electronic documents act Quick reference 2010 Edition, Toronto, Carswell, 2010, p.45.

7.5 Possible Remedies

When PIPEDA is violated, what remedies are available to users?

Section 4.10, Schedule I of PIPEDA provides that "*An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.*"

Thus, a consumer's primary remedy will be to complain directly to the company that collects or uses his personal information. A complaint filed with the Privacy Commissioner of Canada will not be heard if this first step has not been taken.

> *The Commissioner shall conduct an investigation in respect of a complaint, unless the Commissioner is of the opinion that a) the complainant ought first to exhaust grievance or review procedures otherwise reasonably available; (…)*[243]

A consumer whose complaint is not settled to his satisfaction by the "internal remedy" may file his complaint with the Privacy Commissioner of Canada. The latter will determine the complaint's receivability and, if applicable, an investigator will be entrusted with the complaint. Following the investigation, if the Commissioner decides that the complaint is well founded, she will send, to the organization complained about, a draft report including recommendations; the organization will be responsible for explaining to the Commissioner how she plans to implement the recommendations.

It should be noted that the Commissioner has only a power of recommendation, and only the Federal Court can enforce the implementation of those recommendations and award damages.

[243] PIPEDA, section 12 (1) a).

8 Improvement in Cloud Computing Contractual Practices

In this part, we will examine solutions that certain jurisdictions have adopted in two of the three areas we have studied, i.e., consumer protection and privacy. We will focus on the legislative framework and other measures developed abroad, notably in the European Union and the United States, to limit the use, application, scope or effect of certain contractual terms of cloud computing applications. We will consider only the measures that seem most relevant to us, particularly those that are most suitable for being incorporated or adopted in Canadian legislation. We will not detail the measures adopted by each State of the European Union to integrate the European Directives, or the consumer protection laws that may exist in the fifty American states. But we will focus on the measures adopted in France, given the legal history it shares with Quebec. The study of Queen Mary University, which we cited above, discusses cloud computing issues in British law, so we will not detail British law on the subject[244]. We will limit ourselves to mentioning here that study's conclusion: "*Alternatively, public or administrative law intervention or regulatory pressure may be brought to bear against providers to ensure that, for example, European consumers are offered T&C that are compliant with EU consumer law*[245]."

No solution to the problems we raise in our study has been found or implemented abroad with regard to copyright. Accordingly, we will present here no foreign initiative in that regard.

8.1 In Terms of Consumer Protection

In terms of consumer protection, Europe, particularly France, have established specific measures regarding abusive clauses – measures likely to limit the use, scope or effect or some of the contractual clauses we have found problematic.

Before discussing France, it should be recalled that Europe has directives on unfair clauses. Article 3 of Directive 93/13/EEC of April 5, 1993 states that "*A contractual term which has not been individually negotiated shall be regarded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer.*" A list of clauses that may be declared is found in the Directive's Schedule, which has been modified by Directive 2002/995/EC. The means for enforcing the prohibition of those unfair clauses are provided in section 7 of the Directive[246].

[244] Christopher MILLARD & Ian WALDEN, Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services, Queen Mary School of Law Legal Studies Research Paper No. 63/2010 [Online] http://ssrn.com/abstract=1662374 (page consulted on May 11, 2011).
[245] *Ibid.,* p. 46.
[246] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in contracts concluded with consumers, Article 7:
"1. Member States shall ensure that, in the interests of consumers and of competitors, adequate and effective means exist to prevent the continued use of unfair terms in contracts concluded with consumers by sellers or suppliers.
2. The means referred to in paragraph 1 shall include provisions whereby persons or organizations, having a legitimate interest under national law in protecting consumers, may take action according to the national law concerned before the courts or before competent administrative bodies for a decision as to

We recall that European Directives must be ratified by member States. France has amended its consumer code to comply with European requirements. The following focuses on the French provisions.

Section L. 132-1 of France's *Code de la consommation* states:

> *Dans les contrats conclus entre professionnels et non-professionnels ou consommateurs, sont abusives les clauses qui ont pour objet ou pour effet de créer, au détriment du non-professionnel ou du consommateur, un déséquilibre significatif entre les droits et obligations des parties au contrat*[247].

We note that this definition of unfair clauses is similar to that found Quebec law[248]. However, French legislation considers that a clause will be declared unfair as soon as the imbalance it creates is disproportionate, whereas Quebec legislation requires that it be "excessive and unreasonable." Regarding the concept of imbalance, it should be noted that in French law, it "*doit être apprécié […] en fonction de l'équilibre général des prestations réciproques et du principe de la liberté des conventions*[249]."

These provisions on unfair clauses apply in France to cloud computing services. Indeed, Guy Raymond specifies that "*le Code de la consommation ne se préoccupe pas de la nature juridique du contrat. Il peut s'agir d'un contrat de vente ou de prestations de services, d'un contrat de mandat ou de dépôt...*[250]"

To facilitate the work of judges, lists have been developed of clauses presumed or considered unfair. A *Commission des clauses abusives* is charged with recommending "*la suppression ou la modification des clauses qui présentent un caractère abusif*[251]."

In France, consumers are protected in several ways to eliminate unfair contractual clauses. Regulations may impose standard contracts, which necessarily eliminate unfair clauses. Consumers may also go to court, but most importantly, a consumer association may preventively initiate an action for discontinuance of an unfair clause under section L.421-6, subsection 2 of the Code de la consommation[252].

---

whether contractual terms drawn up for general use are unfair, so that they can apply appropriate and effective means to prevent the continued use of such terms.
3. With due regard for national laws, the legal remedies referred to in paragraph 2 may be directed separately or jointly against a number of sellers or suppliers from the same economic sector or their associations which use or recommend the use of the same general contractual terms or similar terms."

[247] Code de la consommation, article L. 132-1.

[248] Section 1437 of the Civil Code of Québec defines as abusive a clause "which is excessively and unreasonably detrimental to the consumer". Section 8 of the Consumer Protection Act considers abusive a clause that creates a "disproportion between the respective obligations of the parties […] so great as to amount to exploitation of the consumer or where the obligation of the consumer is excessive, harsh or unconscionable."

[249] RAYMOND Guy, Clauses abusives, Jurisclasseur Concurrence Consommation, 2005, fascicule 820, p. 17.

[250] *Ibid.,* p. 29.

[251] *Op. Cit.* Note 247, section L. 132-4.

[252] *Op. Cit.* Note 247, article L.421-6: "Les associations mentionnées à l'article L. 421-1 et les organismes justifiant de leur inscription sur la liste publiée au Journal officiel des Communautés européennes en application de l'article 4 de la directive 2009/22/ CE du Parlement européen et du Conseil du 23 avril 2009 relative aux actions en cessation en matière de protection des intérêts des consommateurs peuvent

The Code de la consommation provides criminal sanctions for delinquent merchants. Nevertheless, civil sanctions currently predominate, i.e., voiding of the clause, and damages may be awarded when the consumer can prove that he has suffered prejudice from the application of that unfair clause.

At this time, it should be noted that few laws have considered, in terms of consumer protection, this new phenomenon of cloud computing services. It should also be recognized that current legislation often provides tools that already protect consumers, and that often it would suffice to have such provisions applied strictly and see to it that cloud computing does not escape their application.

In the United States, each state has consumer protection laws. However, there is no measure to protect consumers against unilateral amendments of contracts, for example. Here again, the doctrine of "unconscionability" could find application, including to waiver of liability clauses[253].

Regarding product warranties, the United States has a specific law, the "Magnuson-Moss Warranty Act[254]," that does not, however, apply to services.

It should also be noted that mandatory arbitration clauses are common in the United States.

The most interesting American initiative we find is the "Uniform Computer Information Transactions Act," a federal initiative to create a specific regulatory framework, notably for transactions related to information technologies. But this initiative never became law. In other words, in the United States there are no consumer protection measures that Canada could emulate.

Nevertheless, the Federal Trade Commission may intervene in cases of unfair practices. But for a practice to be deemed unfair, certain conditions must be met: "*in order for a practice to be unfair, the injury it causes must be (1) substantial, (2) without offsetting benefits, and (3) one that consumers cannot reasonably avoid. Each step involves a detailed, fact-specific analysis that must be carefully considered by the Commission*[255]*.*"

agir devant la juridiction civile pour faire cesser ou interdire tout agissement illicite au regard des dispositions transposant les directives mentionnées à l'article 1er de la directive précitée.
Le juge peut à ce titre ordonner, le cas échéant sous astreinte, la suppression d'une clause illicite ou abusive dans tout contrat ou type de contrat proposé ou destiné au consommateur."

[253] ALCES Peter A. and Michael M. GREENFIELD, They can do what!? Limitations on the use of change-of-terms clauses, 26 Georgia State Law University Review (2010) pp. 1133-1134.

[254] United States federal law, 15 U.S.C. § 2301.

[255] BEALES Howard J. The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection, [Online] http://www.ftc.gov/speeches/beales/unfair0603.shtm (page consulted on June 3, 2011).[256] KROES Neelie, The clear role of public authorities in cloud computing, [Online] http://blogs.ec.europa.eu/neelie-kroes/public-authorities-and-cloud/ (page consulted on May 20, 2011).

8.2 In Terms of Personal Information Protection

Cloud computing services clash, in terms of personal information protection, with certain principles established by the OECD Guidelines cited above. Accordingly, the legislative framework and the most important initiatives regarding cloud computing concern the protection of personal information.

First we will discuss what is being done in Europe.

European Union Digital Agenda Commissioner Neelie Kroes has declared on her blog that she has undertaken the development of a European strategy regarding cloud computing. One of the subjects of this strategy is the legal framework:

> ***First, the legal framework***. *This clearly has an international dimension and it concerns for example data protection and privacy, clear rules for the allocation of jurisdiction, responsibility and liability, and consumer protection. Everyone needs clear rights here*[256].

Moreover, it appears that the Commissioner plans to regulate this industry because she estimates that the latter alone cannot, by means of voluntary codes, protect users of this technology[257]. Therefore, a public consultation is underway regarding the legal framework that should apply to this industry.

However, the European regulatory framework already includes certain interesting measures, notably regarding the transfer of personal information. In accordance with Directive 95/46/EC, the European Commission has thus revealed models in the context of its decision of June 15, 2001 regarding standard contractual clauses on the transfer of personal information to third party countries. The decision of December 27, 2004 recalls the existence and importance of those standard contractual clauses. The first recital of that decision perfectly summarizes the reasons why the standard clauses have been developed:

> *In order to facilitate data flows from the Community, it is desirable for data controllers to be able to perform data transfers globally under a single set of data protection rules. In the absence of global data protection standards, standard contractual clauses provide an important tool allowing the transfer of personal data from all Member States under a common set of rules. Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries under Directive 95/46/EC [2] therefore lays down a model set of standard contractual clauses which ensures adequate safeguards for the transfer of data to third countries* [258].

Standard clauses establish a normative framework, so that companies are prohibited from amending those sets of standard clauses. The model set of standard clauses forms a whole; it is impossible to retain only some of the clauses or to eliminate some of them[259].

---

[257] KROES Neelie, The clear role of public authorities in cloud computing, [Online] http ://blogs.ec.europa.eu/neelie-kroes/public-authorities-and-cloud/ (page consulted on May 20, 2011) : "**Why am I making such a big deal of this? Because we can't simply assume that voluntary approaches like codes of conduct will do the job**. Sometimes you need the sort of real teeth only public authorities have." (in bold in the text).

[258] 2004/915/EC: Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries *(notified under document number C(2004) 5271).* Text of interest to the EEA.

[259] *Ibid.*, considering 3.

Those standard clauses specify, for example, the obligations of the data importer. Among those obligations, the data importer must establish appropriate technical and organizational measures to protect personal data, notably from unauthorized access, loss or disclosure of such data. Moreover, the clauses bind subcontractors who might access such data, and who have the same obligations of security and confidentiality. We note that Canadian law includes no provision or requirement of this type; no security or confidentiality obligation is clearly imposed on subcontractors of a foreign company that would itself be a subcontractor or contractee of the Canadian company.

The measures are applied as follows:

> *(…) a data subject shall have the right to enforce as a third party beneficiary this clause and clauses (…) against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter's country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts)*[260].

The consumer has several remedies, against both the exporter and importer, notably when the exporter does not ensure that the importer meets the legal requirements of standard clauses.

In the absence of standard clauses in Canada, it is more difficult for consumers to know the requirements imposed on companies that transfer personal information abroad and on those that import it.

Another community law measure that protects personal information and has no equivalent in Canadian law is noteworthy: the obligation of notification in case of data security risks.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector stipulates in article 4.2:

> *In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.*

Electronic communications services are defined restrictively in article 2 c) of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services:

> c*) "electronic communications service" means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications*

[260] *Ibid.*, article III b).

> *networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks;*

According to this definition, only e-mail services are electronic communications services. Article 4 of the Directive of 2002 was recently reinforced by another Directive (2009/136/EC[261]); considering 59 of this Directive (2009/136/EC) states the amendment's importance:

> *Community law imposes duties on data controllers regarding the processing of personal data, including an obligation to implement appropriate technical and organisational protection measures against, for example, loss of data. The data breach notification requirements contained in Directive 2002/58/EC (Directive on privacy and electronic communications) provide a structure for notifying the competent authorities and individuals concerned when personal data has nevertheless been compromised. Those notification requirements are limited to security breaches which occur in the electronic communications sector. However, the notification of security breaches reflects the general interest of citizens in being informed of security failures which could result in their personal data being lost or otherwise compromised, as well as of available or advisable precautions that they could take in order to minimise the possible economic loss or social harm that could result from such failures. The interest of users in being notified is clearly not limited to the electronic communications sector, and therefore explicit, mandatory notification requirements applicable to all sectors should be introduced at Community level as a matter of priority. Pending a review to be carried out by the Commission of all relevant Community legislation in this field, the Commission, in consultation with the European Data Protection Supervisor, should take appropriate steps without delay to encourage the application throughout the Community of the principles embodied in the data breach notification rules contained in Directive 2002/58/EC (Directive on privacy and electronic communications), regardless of the sector, or the type, of data concerned.*

Under the Directive of 2002 and article 3 of the Directive of 2009 that modifies it, the competent authorities must be notified if confidentiality is violated, but consumers must also be so; henceforth, cloud computing services will also be subject to this obligation.

An entire notification system is put in place to reinforce transparency and consumer confidence. What seems at first sight an absolute obligation is largely tempered: non-notification in case of violation will be authorized if the company has encrypted the data...

> *In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority.*
>
> *When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay.*

[261] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, considering 59, article 2 (Amendments to Directive 2002/58/EC (Directive on privacy and electronic communications).

Notification of a personal data breach to a subscriber or individual concerned shall not be required if the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.

Without prejudice to the provider's obligation to notify subscribers and individuals concerned, if the provider has not already notified the subscriber or individual of the personal data breach, the competent national authority, having considered the likely adverse effects of the breach, may require it to do so.

The notification to the subscriber or individual shall at least describe the nature of the personal data breach and the contact points where more information can be obtained, and shall recommend measures to mitigate the possible adverse effects of the personal data breach. The notification to the competent national authority shall, in addition, describe the consequences of, and the measures proposed or taken by the provider to address, the personal data breach.

In the United States, the *Federal Trade Commission* established in December 2010, following a consultation process, certain measures focusing on targeted advertising, which we have discussed, as well as cloud computing services.

The FTC's principles are the following: first the integration of the concept of "Privacy by Design." Thus, companies should promote the protection of consumers' privacy within their company at each stage of the development of their products and services. Companies should therefore incorporate substantial privacy protection measures in their practices, such as data security, limited data collection, and data accuracy. Moreover, companies should have intelligible data management procedures throughout the useful life of their products and services.

This concept of "Privacy by design," developed by Ann Cavoukian, the Privacy Commissioner of Ontario, is based on seven principles:

The first principle advocates proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen;

The second principle seeks to deliver the maximum degree of privacy;

The third principle is to embed privacy into the design and architecture of IT systems and business practices;

The fourth principle seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner;

The fifth principle, having been embedded into the system prior to the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish;

The sixth principle states that component parts and operations should remain visible and transparent, to users and providers alike;

> *The seventh principle is the most important one: it requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options*[262].

The Article 29 Data Protection working Party has promoted "Privacy by Design" in an Opinion on data protection issues related to search engines[263]. The European Data Protection Supervisor has also promoted "Privacy by Design[264]."

Companies should also simplify the choices offered to consumers regarding the protection of personal information, notably by giving this choice on a timely basis when the consumer will be most able to understand the implications of that choice.

The FTC document mentions a new approach, called "Do Not Track:"

> *One way to facilitate consumer choice is to provide it in a uniform and comprehensive way. Such an approach has been proposed for behavioral advertising, whereby consumers would be able to choose whether to allow the collection and use of data regarding their online searching and browsing activities. The most practical method of providing such universal choice would likely involve the placement of a persistent setting, similar to a cookie, on the consumer's browser signaling the consumer's choices about being tracked and receiving targeted ads. Commission staff supports this approach, sometimes referred to as "Do Not Track*[265]*."*

This solution would enable consumers to express their choices clearly, for instance the choice not to be profiled. This innovative solution seems promising to us.

In addition, companies should improve the transparency of their practices regarding personal data. Privacy policies should be more easily understandable. Standardization would make it possible to compare privacy policies more easily.

An American law firm, InfoLawGroup, has taken the initiative of proposing a "Bill of Rights" for users of cloud computing services[266]. The rights that would be recognized include: the right to know the exact location of data (i.e., their storage location), the right to know precisely what security measures are adopted to protect personal information, the right to be informed of the names of companies that will have access to personal information and to know the purposes for which such access will be accepted, the requirement that companies outsourcing some of their services establish measures guaranteeing that their subcontractors use the same personal information protection measures the outsourcing companies do, and the right to be advised if

[262] See the website Privacy by Design, Information & Privacy Commissioner of Ontario, [Online] http://privacybydesign.ca/ (page consulted on May 20, 2011).
[263] Article 29 Data Protection working Party – Opinion 1/2008 on data protection issues related to search engines, [Online] http://www.cnpd.public.lu/en/publications/groupe-art29/wp148_en.pdf (page consulted on May 20, 2011).
[264] E-waste and data protection: EDPS warns against security risks and calls for "privacy by design," [Online] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2010/EDPS-2010-07_e-waste_EN.pdf (page consulted on May 20, 2011).
[265] Federal Trade Commission, Protection Consumer Privacy in an Era of Rapid Change, December 2010 [Online] www.ftc.gov/os/2010/12/101201privacyreport.pdf (page consulted on May 20, 2011).
[266] NAVETTA David, Cloud Computing Customers' "Bill of Rights," InformationLawGroup, [Online] http://www.infolawgroup.com/2010/10/articles/cloud-computing-1/cloud-computing-customers-bill-of-rights/ (page consulted on May 20, 2011).

confidentiality is breached. The Charter recognizes that consumers' personal information belongs to them and must be used only for specific purposes, and that companies must notify consumers if the authorities access that information. Companies must have procedures for destroying personal information and for the consumer's access to his own personal information.

Since the context likely justifies certain limits, InfoLawGroup did not intend to state absolute rights by listing these basic rights, but rather to lay the foundations of a cloud computing relationship allowing greater transparency, provide users and companies with a tool giving them a better understanding of the potential legal risks of cloud computing, and thus make an informed debate possible[267].

This "Bill of Rights" summarizes well the measures to be taken in order to protect personal information in cloud computing services. Many of the proposals presented there could be integrated in Canadian law to consumers' advantage[268]. They could also serve as a basis for the development of optimal privacy protection standards[269].

[267] *Ibid.*

[268] The United States are considering the adoption of a "Cloud Computer Act," i.e., a specific law for cloud computing. See on this subject MARKS, Joseph, Draft of Cloud Computing Act Sneaks Online. Tech Insider, June 24, 2011. According to the draft made public, the project would focus mainly on applicable civil sanctions in case of unauthorized access to data found in the cloud, [Online] http://techinsider.nextgov.com/2011/06/draft_version_of_cloud_computing_act_is_online.php (page consulted on January 16, 2012).

[269] The Privacy Commissioner, in her report of May 2011, supported in her recommendations the development of such standards. "The OPC urges organizations to develop standards that provide strong security protections. We will continue to track and contribute to work being done by ISO on cloud computing standards." Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing, [Online] http://www.priv.gc.ca/resource/consultations/report_201105_f.cfm (page consulted on May 27, 2011).

Conclusion

Cloud computing is computer technology viewed as a service and externalized. It is a computer model that, by using the memory and calculation capacity of distant computers and servers interconnected by the Internet, enables network access, on demand, to a shared pool of externalized computer resources proposed in the form of services: social networking, e-mail, software, storage space and servers, managed by a third party.

Cloud computing presents five essential characteristics: (*on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service*), four deployment models (private, community, public or hybrid) and three service models: the software service enabling users to benefit from online applications by paying to use the service rather than paying for the software licence; the platform service that enables users to deploy, use and even control applications and other tools on online infrastructures; and the infrastructure service proving users with fundamental computer resources for deploying or using software, applications or operating systems[270]. In the latter case, users control the operating and storage system, but not the service's underlying infrastructure.

Our research aimed primarily to examine cloud computing service contracts under the angle of consumer protection, copyright and privacy protection, in order to verify whether cloud computing services complied with rules established by laws originally intended for services based on tangible space.

To select which cloud computing services to be analysed, we examined the current market of cloud computing services in order to identify the major players, i.e., those providing the services most used by consumers. Several cloud computing services are offered mainly to companies or adapted for them; but we focused on services intended for consumers. Three categories of cloud computing services stood out: e-mail services, data storage services and social networks.

We determined the benefits of cloud computing for consumers: immense calculation and storage capacity available, limiting the need to acquire hardware; capacity to adapt to users' needs; possibility of using the very latest versions of software available on the market (without update fees); possibility of several people working on the same document thanks to increased accessibility; and service reliability reducing the risks of data loss.

Nevertheless, cloud computing does not only present advantages. We identified some of the services' risks or disadvantages, to then verify how legal frameworks could limit them. The risks most often reported pertain to data security – the risk of breaches to data confidentiality. Users fear the loss of data stored in the cloud, but they also fear that stored data can be used by companies for advertising purposes. The fears regarding data security also concern personal information.

Before having access to cloud computing services, the user must provide personal information. That information is gold for cloud computing companies. Using that information, they can do

[270] National Institute of Standards and Technology, Peter Mell & Timothy Grance, The NIST Definition of Cloud Computing (Draft), Special Publication 800-145 [Online] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (page consulted on May 11, 2011).

targeted advertising themselves or allow others to do so by transferring to them the necessary personal information. Targeted advertising is in fact the economic model for cloud computing and the services presented as free by the companies.

One of the difficulties we faced in our research was to legally characterize cloud computing contracts, before being able to determine how various laws apply to them. Finally, we concluded that cloud computing contracts could be legally characterized in several ways: service contracts of successive performance, contracts of successive performance for a service provided at a distance, but also electronic agreements, distance contracts, adhesion contracts and consumer contracts. This last characterization, however, was rejected by a Quebec court estimating that a gratuitous contract could not constitute a consumer contract under the Consumer Protection Act; our analysis convinces us that this characterization should nevertheless apply.

We have observed that the contracts of cloud computing companies often do not comply with Canadian consumer protection legislation. Prohibited clauses, unfair clauses, waiver of liability clauses and warranty exclusion clauses, unilateral amendment or termination clauses, arbitration clauses, choice of forum clauses, clauses stipulating an applicable law other than that of the consumer's residence, automatic renewal clauses – a long list of infractions of the laws of Quebec and Ontario, the provinces chosen for our study.

Regarding copyright, the cloud computing clauses we analysed revealed that the companies draft contracts so as to obtain as many concessions as possible from consumers, who, if they want to use the service, are forced to accept those conditions imposed by a company. Copyright licences that consumers must grant companies are often extremely broad. To determine the economic rights involved, intellectual property licences require great precision; but we rarely find such precision in licences contractually obtained by cloud computing companies. In addition, the licences they impose are intended to be perpetual and irrevocable, whereas civil law prohibits the former characterization, and both the common law and civil law prohibit the latter one.

The problems raised in the light of personal information protection law are many. As we mentioned, the consumer, before having access to cloud computing services, must provide personal information that companies will use notably in targeted advertising. The policies accompanying "requests for consent" or to which the latter refer are too often found in voluminous and complex texts with vague and ambiguous terms that are incomplete, despite the size of the documents – whereas the Act requires transparency in this area.

And yet, it is important that the consumer be informed adequately on the use of his personal information for targeted advertising purposes, but also that he be allowed to actually accept or refuse the use of his personal information for such purposes. 68% of users of at least one cloud computing application say they are very concerned by the fact that the company providing the services can analyse their personal information and then target advertisements to them. Consumer confidence is fragile, and could well drop if the confidentiality of personal information is breached or if such information is used in ways that were not clearly announced or authorized. These risks to the confidentiality of personal information are increased by the fact that cloud computing companies share such information with foreign companies with which they outsource some of the services offered, while outsourcing rules do not necessarily make consumers confident about the security of their personal information.

In the light of all these elements, it is important to assess the risks and problems that cloud computing services pose for consumer protection and to intervene in order to better protect consumers.

In her Report on Online Tracking, Profiling and Targeting, and Cloud Computing, the Privacy Commissioner stated the importance of examining more thoroughly the management of personal information by designers. She pledged to develop guidelines for organizations regarding privacy protection issues in cloud computing, and to develop awareness initiatives intended for consumers using cloud computing services[271]. These are a few of the paths we think should also be explored.

[271] Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing [Online] http://www.priv.gc.ca/resource/consultations/report_201105_e.asp (page consulted on May 27, 2011)

Recommendations

With regard to privacy protection

- **Whereas** to use cloud computing services, Canadian consumers must provide their personal information;
- **Whereas** to finance their cloud computing services, companies collect and use users' personal information for secondary purposes of targeted advertising;

With regard to transparency

- **Whereas** cloud computing companies, although the Personal Information Protection and Electronic Documents Act (PIPEDA) requires them to ensure that precise information on their policies and practices concerning the management of personal information is easily accessible to any person (principle of openness), too often do not disclose to users all their personal information management policies and practices;
- **Whereas**, again according to this principle of openness, cloud computing companies must provide a copy of any brochure or other information document explaining the organization's policy, standards or codes;
- **Whereas** cloud company companies, although PIPEDA requires them to document the purposes for which personal information is collected (principle of identifying purposes), too often do not transparently disclose the purposes of the collection of personal information;
- **Whereas** the personal information management policies of cloud computing companies are long and complex, making them difficult for consumers to read and understand;

With regard users' consent to the collection and use of their personal information

- **Whereas** cloud computing companies, although PIPEDA requires that the person concerned have an opportunity to consent to any collection, use and disclosure of his personal information (principle of consent), too often neglect to give users the necessary means for informed consent to be present;
- **Whereas** cloud computing companies too often do not take all necessary means to ensure consumer confidence in their personal information management policies or practices;

With regard to users' fears

- **Whereas** consumers may be reticent to receive targeted advertising;
- **Whereas** polls reveal that a majority of users would be concerned by the security of contents stored in the cloud, that 90% of users would be very concerned that the company holding their information may sell it to a third party, that 80% of users of cloud computing applications would be very concerned that the companies may use their stored data for advertising purposes, that 68% of users of at least one cloud computing application say they are very worries that the company providing them with those services may analyse their personal information to then target advertisements to them;
- **Whereas** consumers' loss of confidence could imperil the development of cloud computing services intended for them;

With regard to the security of data collected by companies

- **Whereas** PIPEDA requires that personal information be protected by security measures corresponding to its level of sensitivity (principle of security);

- **Whereas** the confidentiality or security of personal information held by cloud computing companies risks being breached;
- **Whereas** companies have no legal obligation to notify the competent authorities, or even the persons concerned, that the confidentiality or security of personal information they keep is or risks being breached;
- **Whereas** the personal information of Canadians are too often transferred abroad by cloud computing companies that outsource some of their services;
- **Whereas** PIPEDA makes companies accountable for personal information they hold or manage, including information transferred to a third party for processing purposes (principle of accountability);
- **Whereas** companies, contractually or otherwise, are obliged to give, to information they transfer to a third party for processing, a level of protection comparable to that imposed PIPEDA;

With regard to possible solutions

- **Whereas** standard clauses for the transfer of personal information abroad have been developed by the European Union;
- **Whereas** the *Federal Trade Commission*, the article 29 Group and the European Data Protection Supervisor, notably, have pleaded in favour of incorporating "Privacy by Design," developed by the Privacy Commissioner of Ontario, as a practice that would help protect personal information, enable cloud computing companies to incorporate in their practices substantial privacy protection measures, such as data security and limits to data collection, and ensure data accuracy;
- **Whereas** a charter of rights has been developed in the United States for users of cloud computing services, as a privacy policy of which many proposals could be integrated in Canadian law to consumers' advantage;
- **Whereas** the *Federal Trade Commission* proposed in December 2010, following a consultation process, a new approach, i.e., that of "Do Not Track," which would allow consumers to clearly express their consent to the secondary use of personal information;
- **Whereas** the standardization of procedures and documents is advocated as a way of promoting the consumer's informed consent;
- **Whereas** the European Union Digital Agenda Commissioner is considering regulation of this industry because she estimates that the industry alone cannot with voluntary codes protect users of this technology;
- **Whereas** the Privacy Commissioner has mentioned the importance of examining more thoroughly the management of personal information by designers, and has pledged to develop guidelines for organizations regarding privacy protection issues in cloud computing, and to develop awareness initiatives intended for consumers using cloud computing services;
- **Whereas** Canadian governments have the power to regulate this area, even when companies providing cloud computing services are abroad;

Union des consommateurs recommends that the federal government:

1. Mandate the Privacy Commissioner of Canada to conduct a thorough investigation of cloud company practices, in view of establishing a uniform framework for the collection and use of Canadians' personal information by cloud computing companies;
2. Amend the Privacy Act to:
   - ensure that all organizations are obliged to report any risk to the security of personal information, as well as any breach of personal information, to the Privacy Commissioner of Canada as well as the individuals whose personal information is the object of such a risk or breach;

- impose standard clauses to cloud computing companies for transferring Canadians personal information to foreign companies;
- impose a “Do not Track” mechanism for targeted advertising;
- incorporate the concept of “Privacy by Design” in that mechanism.

Union des consommateurs recommends that cloud computing companies:

3. make a concerted effort to standardize their procedures and documents regarding privacy protection;
4. pledge greater transparency about their personal information management policies and practices and make a substantial effort to make personal information management policies more understandable to consumers;
5. put in place a “Do not Track” mechanism enabling consumers to clearly make known their choice not to have their personal information used for secondary purposes of targeted advertising;
6. integrate the concept of “Privacy by Design,” in view of ensuring consumer confidence in the protection of personal information;
7. adopt as a privacy policy the “Bill of Rights” developed in the United States.

With regard to copyright:

- **Whereas** cloud computing contracts too often contain excessive and imprecise copyright assignment or licence clauses;
- **Whereas** some copyright assignment or licence clauses may be considered abusive;

Union des consommateurs recommends that companies:

8. clarify copyright assignment or licence clauses, notably regarding the scope of the rights assigned or licenced and the scope of such assignment;

With regard to consumer protection

- **Whereas** the Superior Court of Québec has ruled that gratuitous cloud computing contracts are not subject to the provisions of Quebec’s Consumer Protection Act;
- **Whereas** the provision of personal information by users of those cloud computing services constitutes payment;
- **Whereas** the contracts of cloud computing companies too often contain inapplicable clauses under the Consumer Protection Act, notably arbitration clauses, waiver of liability or warranty exclusion clauses, clauses submitting the contract to foreign laws or jurisdictions, unilateral amendment or termination clauses;
- **Whereas** the contracts of cloud computing companies too often contain unfair or unconscionable clauses, such as waiver of liability clauses in Ontario;
- **Whereas** the Quebec legislature has adopted, in its Consumer Protection Act, provisions regulating unilateral amendments to contracts and requiring contracts to mention the clauses that are inapplicable in this province;
- **Whereas** the Canadian provinces have not harmonized their consumer protection laws in those regards;
- **Whereas** our investigation has identified several cases of cloud companies’ flagrant non-compliance with consumer protection laws;
- **Whereas** provincial laws confer to some individuals or organizations the necessary powers to ensure compliance with consumer protection laws and penalize companies that do not comply with those laws;
- **Whereas** the European Union, particularly France, have developed specific legal frameworks that apply to unfair clauses and that could serve as models for Canadian provincial legislators;

Union des consommateurs recommends that provincial legislators:

9. provide, in provincial consumer protection legislation, a provision clearly indicating that all consumer contracts are subject to consumer protection laws whenever consideration is required of the consumer;
10. impose on merchants the obligation to indicate clearly and explicitly, if applicable, that contractual clauses that are inapplicable under the province's consumer protection act will be void against consumers in that province;
11. strictly regulate merchants' use of unilateral contract amendment clauses;
12. study the possibility and relevance tightening the regulation of unfair clauses, by using as an example the measures adopted in Europe;

Union des consommateurs recommends that organizations responsible for applying consumer protection laws:

13. investigate, in view of sanctioning them, the practices of cloud computing companies that do not comply with the provisions of consumer protection laws.

MEDIAGRAPHY

ADRIVE, Emeryville, California, United States
Privacy Policy, April 8, 2009.
http://www.adrive.com/privacy
Terms of Service, November 22, 2008.
http://www.adrive.com/terms

ALCES Peter A. and Michael M. GREENFIELD, They can do what!? Limitations on the use of change-of-terms clauses, College of William & Mary Law School, Scholarship Repository, Faculty Publications, Paper 279, 48 pages.
http://scholarship.law.wam.edu/cgi/viewcontent.cgi?article=1300&context=facpubs&sei-redir=1#search=%22ALCES+Peter+A.+and+Michael+M.+GREENFIELD,+They+can+do+what!?+Limitations+on+the+use+of+change-of-terms+clauses%22

ARTICLE 29 - DATA PROTECTION WORKING PARTY, Opinion 8/2001 on the processing of personal data in the employment context, European Parliament, website of the Commission nationale pour la protection des données, Luxembourg, Europe, September 13, 2001.
http://www.garanteprivacy.it/garante/document?ID=1365969

BARIBEAU, Marc, *Principes généraux de la Loi sur le droit d'auteur*, Édition 2007, Les publications du Québec, Montreal, 2007.

BAUDOUIN, Jean-Louis and Pierre-Gabriel JOBIN, *Les Obligations*, 5th edition, Éditions Yvon Blais, Cowansville, Quebec, 2005.

BAUDOUIN, Jean-Louis and Yvon Renaud, *Code civil du Québec annoté*, Wilson Lafleur, 12th edition, Quebec, 2009.

BEALES Howard J., *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, site du FTC, Washington, DC, United States, June 25, 2007.
http://www.ftc.gov/speeches/beales/unfair0603.shtm

BRADSHAW Simon, Christopher MILLARD & Ian WALDEN, *Contracts for Clouds: Comparison, and Analysis of the Terms and Conditions of Cloud Computing Services*, Queen Mary School of Law Legal Studies Research Paper No. 63/2010, London, United Kingdom, September 2, 2010. http://ssrn.com/abstract=1662374

BROWNLOW, Mark, Email and webmail statistics, Email Marketing Reports, Vienna, Austria, first publication, April 2008, March 2011 update. http://www.email-marketing-reports.com/metrics/email-statistics.htm

CARLSON, Nicholas, *How Does Facebook Make Money?,* Business Insider, New York, United States, May 18, 2010. http://www.businessinsider.com/how-does-facebook-make-money-2010-5

CHASSIGNEUX, Cynthia, *Vie privée et commerce électronique*, Éditions Thémis, Montreal, Quebec, 2004.

CHASSIGNEUX, Cynthia, *La confiance, instrument de régulation des environnements électroniques*, 37 Revue de droit de l'Université de Sherbrooke, Sherbrooke, Quebec, 2007.

COCHARD, Sandrine, Piratage du PSN : la facture pourrait être salée pour Sony, 20 Minutes, Paris, France, May 10, 2011. http://www.20minutes.fr/article/721359/piratage-psn-facture-pourrait-etre-salee-sony

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing, OPC website, Ottawa, Canada, May 2011. http://www.priv.gc.ca/resource/consultations/report_201105_e.asp

DETURBIDE, Michael, *Consumer Protection Online*, LexisNexis Butterworths, Markham, Ontario, 2006, 180 pages.

DOCTOROW, Cory, *Not every cloud has a silver lining*, Guardian, London, United Kingdom, September 2, 2009. http://www.guardian.co.uk/technology/2009/sep/02/cory-doctorow-cloud-computing

DROPBOX, San Francisco, California, United States,
Terms of Service, 2011.
http://www.dropbox.com/terms
Privacy Policy, 2011.
http://www.dropbox.com/privacy

EDUBOURSE, CAPEX, company website, Brie Comte Robert, France, no date, http://www.edubourse.com/lexique/capex.php

EUROPEAN COMMISSION, The Future of Cloud Computing, Opportunities for European Cloud Computing Beyond 2010, Europa website, Europe, 2010. http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf

FACEBOOK, Canada
Statement of Rights and Responsibilities, October 4, 2010
http://www.facebook.com/terms.php?ref=pf
Data Use Policy, Canada, December 22, 2010.
https://www.facebook.com/policy.php

FEDERAL TRADE COMMISSION, Protection Consumer Privacy in an Era of Rapid Change, site de la FTC, Washington, DC, United States, December 2010. http://www.ftc.gov/os/2010/12/101201privacyreport.pdf

GELLMAN, Robert, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, World Privacy Forum, February 23, 2009. http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf

GFK CUSTOM RESEARCH, GfK Survey: Cloud Computing Has the Power to Enhance Consumer Data Consumption, But Obstacles Hinder Greater Short-Term Adoption, the company's website, New York, NY, United States, March 24, 2011. http://www.gfkamerica.com/newsroom/press_releases/single_sites/007588/index.en.html

GONSALVES, Antone, *Cloud Computing Leaves Consumers Cold*, InformationWeek, San Francisco, California, United States, April 22, 2010.
http://www.informationweek.com/news/hardware/utility_ondemand/224600070

GOOGLE, Mountain View, California, United States,
Privacy Policy, October 3, 2010.
http://www.google.com/intl/en/policies/privacy/
Google Docs Terms of Use, September 2010.
http://www.google.com/google-d-s/intl/en/terms.html
Google Terms of Service, April 16, 2007.
http://www.google.com/intl/en/policies/terms/

GRAND DICTIONNAIRE TERMINOLOGIQUE, definition of cloud computing, website of the Office de la langue française, Montreal, Quebec, 2011.
http://www.granddictionnaire.com/BTML/FRA/r_Motclef/index800_1.asp

HISCOX, Cloud Computing, Hiscox global technology news, Issue 1, Spring, Colchester Essex, United Kingdom, 2011.
http://www.hiscox.co.uk/_HTML_Emails/Group/technology/cloud_comp/usa/

HORRIGAN John, *Use of Cloud Computing Applications and Services*, Pew Internet & American Life Project, Washington, DC, United States, September 12, 2008.
http://www.pewinternet.org/Reports/2008/Use-of-Cloud-Computing-Applications-and-Services/Data-Memo.aspx

IN THE MATTER OF GOOGLE, INC. AND CLOUD COMPUTING SERVICES, Complaint and Request for Injunction, Request for Investigation and for Other Relief Before the Federal Trade Commission, epic.org website, section Cloud Computing, Washington, DC, United States, March 17, 2009.
http://www.google.ca/url?sa=t&source=web&cd=1&ved=0CCIQFjAA&url=http%3A%2F%2Fepic.org%2Fprivacy%2Fcloudcomputing%2Fgoogle%2Fftc031709.pdf&ei=IN7KTer7JYrZgAfLg8zfBQ&usg=AFQjCNFzdWwlvKdQsylcYgBzbuuucUei5Q

INFORMATION & PRIVACY COMMISSIONER OF ONTARIO, Privacy by design, Commissioner's website, Toronto, Ontario, 2011. http://privacybydesign.ca/

JACOBSON, David H., *A view on Cloud Computing*, PricewaterhouseCoopers, company website, Toronto, Ontario, May 2010.
http://www.pwc.com/ca/en/emerging-company/publications/cloud-computing-05-10-en.pdf

JANSEN Wayne and Timothy GRANCE, *Guidelines on Security and Privacy in Public Cloud Computing*, National Institute of Standards and Technology, NSIT website, Draft Special Publication 800-144, Gaithersburg, Washington DC, United States, January 2011.
http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf

KARIM Vincent, *Les obligations*, Volume 1, 3rd edition, Wilson & Lafleur, Montreal, Quebec, 2009, 1525 pages.

KNIGHT Jamie, Sharon CHILCOTT and Melanie McNaught, *Canada Personal information protection and electronic documents act Quick reference 2010 Edition*, Carswell, Toronto, Ontario.

KPMG, Consumers and Convergence IV- Convergence goes Mainstream : Convenience Edges Out Consumer Concerns over privacy and security, KPMG website, Switzerland, July 2010. http://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Pages/Convergence-Goes-Mainstream-O-201007.aspx

KROES Neelie, The clear role of public authorities in cloud computing, blog of the European Commission's Vice-President, Europa website, Europe, 2011. http://blogs.ec.europa.eu/neelie-kroes/public-authorities-and-cloud/

L'HEUREUX Nicole, *Droit de la consommation*, 5th edition, Les Éditions Yvon Blais, Cowansville, Quebec, 2000, 606 pages.

EUROPEAN DATA PROTECTION SUPERVISOR, E-waste and data protection: EDPS warns against security risks and calls for "privacy by design," Press Release, Europa website, Brussels, Belgium, April 15, 2010. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2010/EDPS-2010-07_e-waste_EN.pdf

LLUELLES Didier and Benoît MOORE, *Droit des obligations*, Les éditions Thémis, Montreal, 2006, 2324 pages.

MARCELLIN Sabine, *Cloud computing et risques juridiques,* Legalbiznext, Paris, France, February 2, 2011. http://www.legalbiznext.com/droit/Cloud-computing-et-risques

MARKESS INTERNATIONAL, Cloud Computing & SaaS Attentes et Perspectives, Référentiel de pratiques, 2010 edition, website of Markess international, Paris, France, 2010. http://www.markess.fr/synthese.php

McCAMUS John D., The Law of Contracts, Irwin Law, Toronto, Ontario, August 2005, 1094 pages.

McELROY Griffin, *Class action lawsuit filed against Sony for security breach*, website of Joystiq Network, United States, April 27, 2011. http://www.joystiq.com/2011/04/27/class-action-lawsuit-filed-against-sony-for-security-breach/

McNAIRN Colin H. H., **Alexander Kenny Scott,** A Guide to the Personal Information Protection and Electronic Documents Act, LexisNexis, Butterworths, Markham, Ontario, 2010, 254 pages.

MELL Peter & Timothy GRANCE, *The NIST Definition of Cloud Computing (draft)*, National Institute of Standards and Technology, Special Publication 800-145, National Institute of Standards and Technology, NSIT website, Gaithersburg, Washington DC, United States, January 2011. http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

MICROSOFT, company website, Redmond, Washington, United States,
Microsoft Services Agreement, August 31, 2010.
http://explore.live.com/microsoft-service-agreement?ref=none
Microsoft Online Privacy Statement, November 2010.
http://privacy.microsoft.com/fr-ca/fullnotice.mspx

MOBILEME, Apple website, Cupertino, California, United States,
MobileMe Terms of Service, 2010.
http://www.apple.com/legal/mobileme/en/terms.html
Privacy Policy, June 21, 2010.
http://www.apple.com/privacy/

MOORE Benoît, *Sur l'avenir incertain du contrat de consommation*, Les Cahiers de droit, Vol. 49, No. 1, Université Laval, Quebec, 2008,
http://www.fd.ulaval.ca/site/cms/affichage.php?page=../cahiers/vol49no1.php&menu=269

NAVETTA David, Cloud Computing Customers' "Bill of Rights," InformationLawGroup, New York, United States, October 11, 2010. http://www.infolawgroup.com/2010/10/articles/cloud-computing-1/cloud-computing-customers-bill-of-rights/

NEUMUELLER Carina, *Are We "There" Yet? An Analysis of Canadian and European Adjudicatory Jurisdiction Principles in the Context of Electronic Commerce Consumer*, Vol. 3, No. 2, University of Ottawa Law and Technology Journal, University of Ottawa, Ottawa, Ontario, 2006, pages 421-456. http://www.uoltj.ca/articles/vol3.2/2006.3.2.uoltj.Neumueller.421-456.pdf

O'NEILL Nick, The Secret to How Facebook Makes Money, All Facebook- The Unofficial Facebook Resource, United States, January 19, 2010.
http://www.allfacebook.com/facebook-makes-money-2010-01

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, OECD Council Recommendation regarding Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD website, Paris, France, September 23, 1980.
http://www.oecd.org/document/18/0,3746,en_2649_34223_1815186_1_1_1_1,00.html

Horrigan, John B. Associate Director, Use of Cloud Computing applications and services, site de Pew Internet & American Life Project, Washington, DC, United States, September 2008.
http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Cloud.Memo.pdf.pdf

RANSOM-WILEY James, Canadian firm proposes class action against Sony to the tune of $1B in damages, website of Joystiq Network, United States, May 4, 2011.
http://www.joystiq.com/2011/05/04/canadian-firm-proposes-class-action-against-sony-to-the-tune-of/

RAYMOND Guy, *Clauses abusives*, Jurisclasseur Concurrence Consommation, fascicule 820, Paris, France, 2005.

RAYPORT Jeffrey F. & Andrew HEYWARD, *Marketspace Point of view, Envisioning the Cloud: The Next Computing Paradigm*, on the company's website, United States, March 20, 2009. http://marketspacenext.files.wordpress.com/2011/01/envisioning-the-cloud.pdf

ROBISON William J., *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 The Georgetown Law Journal 1195, Washington, DC, United States, 2010, 45 pages.
http://www.georgetownlawjournal.com/issues/pdf/98-4/Robison.PDF

SCHICK Shane, *Five ways of defining cloud computing,* it World Canada, Scarborough, Ontario Canada, April 22, 2008.
http://www.itworldcanada.com/blogs/shane/2008/04/22/five-ways-of-defining-cloud-computing/48746/

SHIELDS Simon, Consumer law, Part C, Consumer Protection (Ontario) Law, isthatlegal.ca website, Toronto, Ontario, March 30, 2010.
http://www.isthatlegal.ca/index.php?name=civil_remedies1.consumer_protection_law_ontario#Overview

SVANTESSON Dan and Roger CLARKE, *Privacy and Consumer risks on cloud computing*, 26(4) Computer law and security review, on the website of epublications.bond.edu.au, pp. 391-397, Australia, July 1, 2010. http://epublications.bond.edu.au/law_pubs/347

SWAN Angela, Canadian Contract Law, 2nd edition, Lexis Nexis, Markham, Ontario, 2009, 1051 pages.

SYNTEC NUMÉRIQUE, Livre Blanc Sécurité du Cloud Computing, Analyse des risques, réponses et bonnes pratiques, Paris, France, May 5, 2010.
http://www.syntec-numerique.fr/actualites/liste-actualites/livre-blanc-cloud-computing-securite

TAMARO Normand, Loi sur le droit d'auteur, 6th edition, Thomson Carswell, Scarborough, Ontario, 2003,

WIKIPEDIA, collective encyclopedia, United States
Cloud computing, 2011.
http://en.wikipedia.org/wiki/Cloud_computing#History
Customer relationship management, 2011.
http://en.wikipedia.org/wiki/Customer_relationship_management
Operating expense, 2011.
https://secure.wikimedia.org/wikipedia/en/wiki/Operating_expense

YAHOO!, company website
Security at Yahoo!, United States, 2011.
http://info.yahoo.com/privacy/us/yahoo/security/
Terms of Service, Canada, 2011.
http://info.yahoo.com/legal/ca/yahoo/utos/utos-ca01.html
Yahoo! Privacy Policy, Canada, April 23, 2010.
http://info.yahoo.com/privacy/ca/yahoo/

ZOHO, Pleasanton, California, United States,
Privacy Policy, December 28, 2010.
http://www.zoho.com/privacy.html
Terms of Services, April 16, 2010.
http://www.zoho.com/terms.html

ZUMODRIVE, United States,
Privacy Policy, September 1, 2010.
http://www.zumodrive.com/privacy
Terms of Service, 2011.
http://www.zumodrive.com/tos

ANNEX 1 Adrive – Terms of Service

TERMS OF SERVICE

http://www.adrive.com/terms

(Last Updated: November 22, 2008)

B. Terms and Conditions.

3. Your Identity. You agree to provide Adrive with accurate, timely information about Yourself and/or the minor over the age of 13 on whose behalf You are entering this Agreement, and update Your contact data such that it remains current. You will not provide Adrive with false information about Your identity, impersonate another person or entity, or otherwise misrepresent Your identity or affiliation to Adrive. Adrive will use that information only in a manner consistent with that disclosed in Adrive's Privacy Policy, which is incorporated into this Agreement by reference. Your failure to comply with this provision automatically nullifies any obligation Adrive may have to contact You or provide You with any notice required by this Agreement or by law.

15. DISCLAIMER OF WARRANTIES. ADRIVE'S SERVICES AND MATERIALS AND THIRD PARTY CONTENT ACCESSIBLE IN CONNECTION THEREWITH ARE PROVIDED "AS IS" AND "AS AVAILABLE", AND, EXCEPT AS EXPRESSLY PROVIDED HEREIN, WITHOUT WARRANTIES OF ANY KIND. TO THE FULLEST EXTENT PERMISSIBLE BY APPLICABLE LAW, ADRIVE DISCLAIMS ALL SUCH WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Without limiting the generality of the foregoing, Adrive does not warrant that the functions and/or services of Adrive-related services, Storage Data, hardware, sites, software, data or other material will be uninterrupted or error-free, or that defects will be detected or corrected; neither Adrive nor any third party Storage Data provider warrants that any service, software, Storage Data or the methods by which they are made available will be free of viruses or similar contamination or destructive features. You expressly agree to solely assume the entire risk as to the quality and performance of Adrive's services and the accuracy or completeness of Storage Data. Adrive does not warrant or make any representations regarding the use or the results of the use of its services, software, Storage Data, the materials, functions, data or services in or provided by Adrive, its affiliates or its Users in terms of accuracy, reliability, or otherwise. You expressly agree to assume the entire cost of all necessary servicing, repair, correction and related liabilities resulting from Your use of Adrive's services. If applicable law does not allow the exclusion of implied warranties, certain of the above exclusion may not apply to You.

16. LIMITATION OF LIABILITY. YOU AGREE THAT, EXCEPT AS OTHERWISE EXPRESSLY PROVIDED IN THIS AGREEMENT, UNDER NO CIRCUMSTANCES, INCLUDING (BUT NOT LIMITED TO) NEGLIGENCE, SHALL ADRIVE BE LIABLE FOR ANY DAMAGES (INCLUDING, BUT NOT LIMITED TO, DIRECT, ACTUAL, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES) THAT RELATE TO OR RESULT FROM THE USE OF, THE INABILITY TO USE, OR THE CORRUPTION OF STORAGE DATA, OR OTHER DATA STORED ON, STORED IN, RETRIEVED FROM, ACQUIRED, TRANSMITTED OR TRANSFERRED THROUGH ADRIVE'S SERVICES, EVEN IF ADRIVE OR ITS

REPRESENTATIVES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL ADRIVE'S AGGREGATE LIABILITY TO YOU ANY USER DESIGNATED BY YOU FOR ALL DAMAGES, LOSSES, AND CAUSES OF ACTION (WHETHER IN CONTRACT, TORT (INCLUDING, BUT NOT LIMITED TO, NEGLIGENCE), OR OTHERWISE) EXCEED THE GREATER OF U.S. $100 OR THE AMOUNT ACTUALLY PAID BY YOU FOR ACCESSING THIS SITE. If applicable law does not allow the limitation or exclusion of liability or incidental or consequential damages, certain of the above limitations or exclusions may not apply to You.

18. Termination for Convenience. Adrive reserves the right to change, suspend or discontinue all or any aspect of its services made available to You or others at any time, including the availability of any feature, Storage Data, without prior notice or liability to You. Either party may terminate this Agreement at any time for any reason or for no reason by sending notice of termination to the other party. You expressly waive and release Adrive from any and all claims You may have against Adrive arising out of or related to any such termination.

20. Choice of Law and Venue. Adrive's services are managed from its offices within the State of California, United States of America. Adrive makes no representation that its services are appropriate or available for use in other locations. If You choose to access this site from other locations, You do so on Your own initiative and are responsible for compliance with local laws, if and to the extent local laws are applicable. All matters with respect to this Agreement, including, without limitation, matters of validity, construction, effect and performance shall be governed by the internal laws of the State of California applicable to contracts made and to be performed therein between the residents thereof (regardless of the laws that might otherwise be applicable under principles of conflicts of law). Any action or proceeding related to the subject matter of this Agreement shall be venued in San Francisco, California. You hereby agree to submit to personal jurisdiction in the federal and state courts located in San Francisco, California. This Agreement shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods.

23. Modifications. Adrive may from time to time amend the terms and conditions of this Agreement. At the time of any such change, You will be notified of the modified terms and conditions. Continued use of Adrive's services after the effective date of the notification shall constitute acceptance of the changed Agreement.

25. Arbitration. Any dispute between You and Adrive relating to this Agreement, Storage Data or Adrive's services, hardware or software shall be resolved by binding arbitration pursuant to the commercial rules of the American Arbitration Association. Any such controversy or claim shall be arbitrated on an individual basis, and shall not be consolidated in any arbitration with any claim or controversy of any other party. The arbitration shall be conducted in San Francisco, California, and any judgment on the arbitration award may be entered in any court having jurisdiction thereof.

ANNEX 2 Adrive – Privacy Policy

ADRIVE PRIVACY POLICY

http://www.adrive.com/privacy

(Last Updated: April 8, 2009)

This Privacy Policy statement discloses ADrive's information sharing practices and is incorporated into and is subject to the ADrive Terms of Use. By entering into the Agreement, you expressly consent to ADrive's use and disclosure of Your personal information in accordance with this Privacy Policy.

a. Information Collection and Use. ADrive is the sole owner of the information collected from its Users. Except as required by law, subpoena or court order, ADrive will not sell, share, or rent this information to others except as permitted by this policy.

b. Registration. In order to use ADrive's services, Users must first complete a registration form, which requires providing ADrive certain information. This information is used to identify the specific User utilizing ADrive's services. The User may provide optional identifying information, demographic information, and unique identifiers to enable us to provide a more personalized experience on the site.

g. Use of Personal Information. ADrive will not give, sell, rent, share, or trade any personal information about You to third parties or provide Your personal information, including your name or electronic mail address, to third parties except as required by law, subpoena or court order. ADrive may disclose Your username, name, address, electronic mail, and other personal information as it believes necessary or appropriate in connection with an investigation for fraud, intellectual property infringement, piracy, or other illegal activity as well as dispute resolution and enforcement of the Agreement. ADrive will share aggregated demographic information with its partners and advertisers. This is not linked to any personal information that can identify any individual person.

j. Security. ADrive uses available best practices to protect our Users' information. When ADrive asks users to enter sensitive information (such as credit card number), that information is protected with SSL encryption software for transmission to ADrive. All of our Users' information is restricted in our offices. Only employees or contractors who need the information to perform a specific job are granted access to personally identifiable information

o. Choice/Opt-out. You may opt-out of having Your information used for purposes not directly related to ADrive's services at the point where we ask for the information. Users who no longer wish to receive promotional materials from our partners may opt-out of receiving these communications by replying with unsubscribe in the subject line in the electronic mail or electronic mail us at support@adrive.com.

r. Advertising. We use third-party advertising companies to serve ads when you visit our website. These companies may use information (not including your name, address, email address, or telephone number) about your visits to this and other websites in order to provide advertisements about goods and services of interest to you. If you would like more information about this practice and to know your choices about not having this information used by these companies, click here.

ANNEX 3 Dropbox – Terms of Service

DROPBOX TERMS OF SERVICE

http://www.dropbox.com/terms

Files and Folders
"***Your Files***" or "***User Files***" (collectively, the "***Files***") as used in this Agreement means the information contained in the files that you or other users upload, download and access through the Site and Services. You are the owner of Your Files and are solely responsible for your conduct and the content of Your Files, as well as any of the content contained in your communications with other Dropbox users, including but not limited to User Posts (as defined below).

Dropbox allows you to share some or all of Your Files. If you choose to, you can share all or some of Your Files with the general public, or with specific individuals you select. If you decide to share Your Files, you are giving certain legal rights, as explained below, to those individuals who you have given access to your folders.

Dropbox does not claim any ownership rights in Your Files. You acknowledge that Dropbox does not have any obligation to monitor the Files or User Posts that are uploaded, posted, submitted, linked to or otherwise transmitted using the Site or Services, for any purpose and, as a result, is not responsible for the accuracy, completeness, appropriateness, legality or applicability of the Files or anything said, depicted or written by users in their User Posts, including without limitation, any information obtained by using the Site or Services. Dropbox does not endorse anything contained in the Files or User Posts or any opinion, recommendation or advice expressed therein and you agree to waive, and hereby do waive, any legal or equitable rights or remedies you have or may have against Dropbox with respect thereto.

Your Public Folder
While you own the content contained in Your Files, files placed in your public folders are automatically available to other Dropbox users and to the general public. By placing Your Files in your public folder, you hereby grant all other Dropbox users and the public a non-exclusive, non-commercial, worldwide, royalty-free, sublicensable, perpetual and irrevocable right and license to use and exploit Your Files in your public folder. In other words, a file in your public folder can be used by anyone, for any purpose *except* commercial use. If you do not want other people to be able to use Your Files in this manner, then simply do not place Your Files in your public folder. By placing Your Files in your public folder, you agree and acknowledge that Dropbox has no responsibility or obligation to monitor or notify of you of any non-compliance related to the license you have granted and that Dropbox has no responsibility to enforce or police, or aid you in enforcing or policing, the terms of that license.

Your Shared Folder
While you own the content contained in Your Files, files placed in your shared folders are available to those users to whom you grant access. By placing Your Files in your shared folder, you agree and acknowledge that Dropbox has no responsibility or obligation to monitor or notify of you of any non-compliance related to the rights or license you may choose to grant to other users who have access to your shared folders, if any, and that Dropbox has no responsibility to

enforce or police, or aid you in enforcing or policing, the terms of the license(s) or permission(s) you have chosen to offer.

Termination
If you violate any of these Terms of Service, your permission to use the Site, Content**,** Files and Services will automatically terminate. Dropbox reserves the right to revoke your access to and use of the Site, Content, Files and Services at any time, with or without cause, and with or without notice. Dropbox also reserves the right to cease providing or to change the Site, Content, Files or Services at any time and without notice.

Dropbox reserves the right to terminate Free Accounts at any time, with or without notice. Without limiting the generality of the foregoing, and without further notice, Dropbox may choose to delete and/or reduce: (i) any or all of Your Files if your Free Account is inactive for 90 days; and (ii) previous versions and/or prior backups of Your Files.

Dropbox is Available "AS-IS"
THE SITE, CONTENT, FILES AND SERVICES ARE PROVIDED "AS IS", WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. WITHOUT LIMITING THE FOREGOING, DROPBOX EXPLICITLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT AND ANY WARRANTIES ARISING OUT OF COURSE OF DEALING OR USAGE OF TRADE. YOU ACKNOWLEDGE THAT USE OF THE SITE, CONTENT, FILE AND SERVICES MAY RESULT IN UNEXPECTED RESULTS, LOSS OR CORRUPTION OF DATA OR COMMUNICATIONS, PROJECT DELAYS, OTHER UNPREDICTABLE DAMAGE OR LOSS, OR EXPOSURE OF YOUR DATA OR YOUR FILES TO UNINTENDED THIRD PARTIES.

DROPBOX MAKES NO WARRANTY THAT THE SITE, CONTENT, FILES OR SERVICES WILL MEET YOUR REQUIREMENTS OR BE AVAILABLE ON AN UNINTERRUPTED, SECURE, OR ERROR-FREE BASIS. DROPBOX MAKES NO WARRANTY REGARDING THE QUALITY OF ANY PRODUCTS, SERVICES, OR INFORMATION PURCHASED OR OBTAINED THROUGH THE SITE, CONTENT**,** OR SERVICES, OR THE ACCURACY, TIMELINESS, TRUTHFULNESS, COMPLETENESS OR RELIABILITY OF ANY INFORMATION OBTAINED THROUGH THE SITE, CONTENT**,** FILES OR SERVICES.

NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED FROM DROPBOX OR THROUGH THE SITE, CONTENT**,** FILES OR SERVICES, WILL CREATE ANY WARRANTY NOT EXPRESSLY MADE HEREIN.

Limitation of Liability
IN NO EVENT WILL DROPBOX BE LIABLE TO YOU OR TO ANY THIRD PARTY FOR DAMAGES OF ANY KIND, INCLUDING, WITHOUT LIMITATION, DIRECT, SPECIAL, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES (INCLUDING LOSS OF USE, DATA, BUSINESS OR PROFITS) ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT, OR FROM YOUR ACCESS TO OR USE OF, OR INABILITY TO ACCESS OR USE, THE SITE, CONTENT, FILES AND/OR SERVICES, OR FOR ANY ERROR OR DEFECT IN THE SITE, CONTENT**,** FILES OR SERVICES, WHETHER SUCH LIABILITY ARISES FROM ANY CLAIM BASED UPON CONTRACT, WARRANTY, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, OR ANY OTHER LEGAL THEORY, WHETHER OR NOT DROPBOX HAS BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGE, EVEN IF A REMEDY SET FORTH HEREIN IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE. YOU SPECIFICALLY ACKNOWLEDGE THAT DROPBOX IS NOT LIABLE FOR THE

DEFAMATORY, OFFENSIVE OR ILLEGAL CONDUCT OF OTHER USERS OR THIRD PARTIES AND THAT THE RISK OF INJURY FROM THE FOREGOING RESTS ENTIRELY WITH YOU. FURTHER, DROPBOX WILL HAVE NO LIABILITY TO YOU OR TO ANY THIRD PARTY FOR ANY THIRD PARTY CONTENT UPLOADED ONTO OR DOWNLOADED FROM THE SITE OR THROUGH THE SERVICES AND/OR THE FILES, OR IF YOUR DATA IS LOST, CORRUPTED OR EXPOSED TO UNINTENDED THIRD PARTIES.

FREE ACCOUNT HOLDERS: YOU AGREE THAT THE AGGREGATE LIABILITY OF DROPBOX TO YOU FOR ANY AND ALL CLAIMS ARISING FROM THE USE OF THE SITE, CONTENT, FILES AND/OR SERVICES IS LIMITED TO TWENTY ($20) U.S. DOLLARS. THE LIMITATIONS OF DAMAGES SET FORTH ABOVE ARE FUNDAMENTAL ELEMENTS OF THE BASIS OF THE BARGAIN BETWEEN DROPBOX AND YOU.

PREMIUM ACCOUNT HOLDERS: YOU AGREE THAT THE AGGREGATE LIABILITY OF DROPBOX TO YOU FOR ANY AND ALL CLAIMS ARISING FROM THE USE OF THE SITE, CONTENT, FILES AND/OR SERVICES IS LIMITED TO LOWER OF THE AMOUNTS YOU HAVE PAID TO DROPBOX DURING THE THREE MONTH PERIOD PRIOR TO SUCH CLAIM, FOR ACCESS TO AND USE OF THE SITE, CONTENT**,** FILES OR SERVICES, OR ONE-HUNDRED ($100) DOLLARS. THE LIMITATIONS OF DAMAGES SET FORTH ABOVE ARE FUNDAMENTAL ELEMENTS OF THE BASIS OF THE BARGAIN BETWEEN DROPBOX AND YOU.

Controlling Law and Jurisdiction
These Terms of Service and any action related thereto will be governed by the laws of the State of California without regard to its conflict of law provisions. The exclusive jurisdiction and venue of any action with respect to the subject matter of these Terms of Service will be the state and federal courts located in San Francisco County, California, and each of the parties hereto waives any objection to jurisdiction and venue in such courts.

ANNEX 4 Dropbox – Privacy Policy

DROPBOX PRIVACY

Dropbox provides this Privacy Policy to inform you of our policies and procedures regarding the collection, use and disclosure of personal information we receive from users of www.dropbox.com (this "***Site***"). This Privacy Policy applies only to information that you provide to us through this Site. Our Privacy Policy may be updated from time to time, and we will notify you of any material changes by posting the new Privacy Policy on the Site at http://www.dropbox.com/privacy

1. Information Collection: The Personally Identifiable Information We Collect
In the course of using this Site, you may provide us with personally identifiable information. This refers to information about you that can be used to contact or identify you, and information on your use of and activities at our Site that may be connected with you ("***Personal Information***"). Personal Information that we collect may include, but is not limited to, your name, phone number, credit card or other billing information, email address and home and business postal addresses. Personal Information may also include information you supply to us concerning your preferences and interests expressed in the course of use of our Site.

When you visit the Site, our servers automatically record information that your browser sends whenever you visit a website. This information may include, but is not limited to, your computer's Internet Protocol address, browser type, the web page you were visiting before you came to our Site and information you search for on our Site. Like many websites, we may also use "cookies" to collect information. A cookie is a small data file that we transfer to your computer's hard disk for record-keeping purposes. We may use "persistent cookies" to save your registration ID and login password for future logins to the Site; and we use "session ID cookies" to enable certain features of the Site, to better understand how you interact with the Site and to monitor aggregate usage and web traffic routing on the Site. You can instruct your browser, by changing its options, to stop accepting cookies or to prompt you before accepting a cookie from the websites you visit. If you do not accept cookies, however, you may not be able to use all portions of the Site or all functionality of our services.

2. How We Use Personal Information
Personal Information is or may be used for the following purposes: (i) to provide and improve our Site, services, features and content, (ii) to administer your use of our Site, (iii) to enable you to enjoy and easily navigate the Site, (iv) to better understand your needs and interests, (v) to fulfill requests you may make, (vi) to personalize your experience, (vii) to provide or offer software updates and product announcements, and (viii) to provide you with further information and offers from us or third parties that we believe you may find useful or interesting, including newsletters, marketing or promotional materials and other information on services and products offered by us or third parties. If you decide at any time that you no longer wish to receive any such communications, please follow the "unsubscribe" instructions provided in any of the communications sent to you, or update your "account settings" information. (See "**Changing or Deleting Information**," below.)

We use information we obtain by technical means (such as the automatic recording performed by our servers or through the use of cookies) for the above purposes and in order to monitor

and analyze use of the Site and our services, for the Site's technical administration, to increase our Site's functionality and user-friendliness, to better tailor it to your needs, to generate and derive useful data and information concerning the interests, characteristics and website use behavior of our users, and to verify that visitors to the Site meet the criteria required to process their requests.

3. Information Sharing and Disclosure
Dropbox Users. We will display your Personal Information in your profile page and elsewhere on the Site according to the preferences you set in your account. Any information you choose to provide should reflect how much you want other Dropbox users to know about you. We recommend that you guard your anonymity and sensitive information, and we encourage users to think carefully about what information about themselves they disclose in their profile pages. You can review and revise your profile information at any time.

Service Providers, Business Partners and Others. We may employ third party companies and individuals to facilitate our service, to provide the service on our behalf, to perform Site-related services (including but not limited to data storage, maintenance services, database management, web analytics, payment processing, and improvement of the Site's features) or to assist us in analyzing how our Site and service are used. These third parties have access to your Personal Information only for purposes of performing these tasks on our behalf.

Compliance with Laws and Law Enforcement. Dropbox cooperates with government and law enforcement officials and private parties to enforce and comply with the law. We will disclose any information about you to government or law enforcement officials or private parties as we, in our sole discretion, believe necessary or appropriate to respond to claims and legal process (including but not limited to subpoenas), to protect the property and rights of Dropbox or a third party, to protect the safety of the public or any person, or to prevent or stop any activity we may consider to be, or to pose a risk of being, illegal, unethical, inappropriate or legally actionable.

Business Transfers. Dropbox may sell, transfer or otherwise share some or all of its assets, including your Personal Information, in connection with a merger, acquisition, reorganization or sale of assets or in the event of bankruptcy.

5. Security
Dropbox is very concerned with safeguarding your information. We employ reasonable measures designed to protect your information from unauthorized access.

ANNEX 5 Facebook – Statement of Rights and Responsibilities

FACEBOOK

http://www.facebook.com/terms.php?ref=pf

This agreement was written in English (US). To the extent any translated version of this agreement conflicts with the English version, the English version controls. Please note that Section 16 contains certain changes to the general terms for users outside the United States.

Date of Last Revision: April 26, 2011.

Statement of Rights and Responsibilities

This Statement of Rights and Responsibilities (Statement) derives from the Facebook Principles, and governs our relationship with users and others who interact with Facebook. By using or accessing Facebook, you agree to this Statement.

1. **Privacy**

   Your privacy is very important to us. We designed our Privacy Policy to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information. We encourage you to read the Privacy Policy, and to use it to help make informed decisions.

2. **Sharing Your Content and Information**

   You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings. In addition:

   a. For content that is covered by intellectual property rights, like photos and videos (IP content), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it.
   b. When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be available to others).
   c. When you use an application, your content and information is shared with the application. We require applications to respect your privacy, and your agreement with that application will control how the application can use, store, and transfer that content and information. (To learn more about Platform, read our Privacy Policy and Platform Page.)

d. When you publish content or information using the Public setting, it means that you are allowing everyone, including people off of Facebook, to access and use that information, and to associate it with you (i.e., your name and profile picture).
e. We always appreciate your feedback or other suggestions about Facebook, but you understand that we may use them without any obligation to compensate you for them (just as you have no obligation to offer them).

3. **Safety**

We do our best to keep Facebook safe, but we cannot guarantee it. We need your help to do that, which includes the following commitments:

a. You will not send or otherwise post unauthorized commercial communications (such as spam) on Facebook.
b. You will not collect users' content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without our permission.
c. You will not engage in unlawful multi-level marketing, such as a pyramid scheme, on Facebook.
d. You will not upload viruses or other malicious code.
e. You will not solicit login information or access an account belonging to someone else.
f. You will not bully, intimidate, or harass any user.
g. You will not post content that: is hateful, threatening, or pornographic; incites violence; or contains nudity or graphic or gratuitous violence.
h. You will not develop or operate a third-party application containing alcohol-related or other mature content (including advertisements) without appropriate age-based restrictions.
i. You will follow our Promotions Guidelines and all applicable laws if you publicize or offer any contest, giveaway, or sweepstakes (“promotion”) on Facebook.
j. You will not use Facebook to do anything unlawful, misleading, malicious, or discriminatory.
k. You will not do anything that could disable, overburden, or impair the proper working of Facebook, such as a denial of service attack.
l. You will not facilitate or encourage any violations of this Statement.

4. **Registration and Account Security**

Facebook users provide their real names and information, and we need your help to keep it that way. Here are some commitments you make to us relating to registering and maintaining the security of your account:

a. You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission.
b. You will not create more than one personal profile.
c. If we disable your account, you will not create another one without our permission.
d. You will not use your personal profile for your own commercial gain (such as selling your status update to an advertiser).
e. You will not use Facebook if you are under 13.
f. You will not use Facebook if you are a convicted sex offender.

g. You will keep your contact information accurate and up-to-date.
h. You will not share your password, (or in the case of developers, your secret key), let anyone else access your account, or do anything else that might jeopardize the security of your account.
i. You will not transfer your account (including any page or application you administer) to anyone without first getting our written permission.
j. If you select a username for your account we reserve the right to remove or reclaim it if we believe appropriate (such as when a trademark owner complains about a username that does not closely relate to a user's actual name).

10. About Advertisements and Other Commercial Content Served or Enhanced by Facebook

Our goal is to deliver ads that are not only valuable to advertisers, but also valuable to you. In order to do that, you agree to the following:

1. You can use your privacy settings to limit how your name and profile picture may be associated with commercial, sponsored, or related content (such as a brand you like) served or enhanced by us. You give us permission to use your name and profile picture in connection with that content, subject to the limits you place.
2. We do not give your content or information to advertisers without your consent.
3. You understand that we may not always identify paid services and communications as such.

13. Amendments

1. We can change this Statement if we provide you notice (by posting the change on the Facebook Site Governance Page) and an opportunity to comment. To get notice of any future changes to this Statement, visit our Facebook Site Governance Page and become a fan.
2. For changes to sections 7, 8, 9, and 11 (sections relating to payments, application developers, website operators, and advertisers), we will give you a minimum of three days notice. For all other changes we will give you a minimum of seven days notice. All such comments must be made on the Facebook Site Governance Page.
3. If more than 7,000 users comment on the proposed change, we will also give you the opportunity to participate in a vote in which you will be provided alternatives. The vote shall be binding on us if more than 30% of all active registered users as of the date of the notice vote.
4. We can make changes for legal or administrative reasons, or to correct an inaccurate statement, upon notice without opportunity to comment.

14. Termination

If you violate the letter or spirit of this Statement, or otherwise create risk or possible legal exposure for us, we can stop providing all or part of Facebook to you. We will notify you by email or at the next time you attempt to access your account. You may also delete your account or disable your application at any time. In all such cases, this Statement shall terminate, but the following provisions will still apply: 2.2, 2.4, 3-5, 8.2, 9.1-9.3, 9.9, 9.10, 9.13, 9.15, 9.18, 10.3, 11.2, 11.5, 11.6, 11.9, 11.12, 11.13, and 14-18.

15. Disputes

1. You will resolve any claim, cause of action or dispute (claim) you have with us arising out of or relating to this Statement or Facebook exclusively in a state or federal court located in Santa Clara County. The laws of the State of California will govern this Statement, as well as any claim that might arise between you and us, without regard to

conflict of law provisions. You agree to submit to the personal jurisdiction of the courts located in Santa Clara County, California for the purpose of litigating all such claims.

2. If anyone brings a claim against us related to your actions, content or information on Facebook, you will indemnify and hold us harmless from and against all damages, losses, and expenses of any kind (including reasonable legal fees and costs) related to such claim.
3. WE TRY TO KEEP FACEBOOK UP, BUG-FREE, AND SAFE, BUT YOU USE IT AT YOUR OWN RISK. WE ARE PROVIDING FACEBOOK AS IS WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. WE DO NOT GUARANTEE THAT FACEBOOK WILL BE SAFE OR SECURE. FACEBOOK IS NOT RESPONSIBLE FOR THE ACTIONS, CONTENT, INFORMATION, OR DATA OF THIRD PARTIES, AND YOU RELEASE US, OUR DIRECTORS, OFFICERS, EMPLOYEES, AND AGENTS FROM ANY CLAIMS AND DAMAGES, KNOWN AND UNKNOWN, ARISING OUT OF OR IN ANY WAY CONNECTED WITH ANY CLAIM YOU HAVE AGAINST ANY SUCH THIRD PARTIES. IF YOU ARE A CALIFORNIA RESIDENT, YOU WAIVE CALIFORNIA CIVIL CODE §1542, WHICH SAYS: A GENERAL RELEASE DOES NOT EXTEND TO CLAIMS WHICH THE CREDITOR DOES NOT KNOW OR SUSPECT TO EXIST IN HIS FAVOR AT THE TIME OF EXECUTING THE RELEASE, WHICH IF KNOWN BY HIM MUST HAVE MATERIALLY AFFECTED HIS SETTLEMENT WITH THE DEBTOR. WE WILL NOT BE LIABLE TO YOU FOR ANY LOST PROFITS OR OTHER CONSEQUENTIAL, SPECIAL, INDIRECT, OR INCIDENTAL DAMAGES ARISING OUT OF OR IN CONNECTION WITH THIS STATEMENT OR FACEBOOK, EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. OUR AGGREGATE LIABILITY ARISING OUT OF THIS STATEMENT OR FACEBOOK WILL NOT EXCEED THE GREATER OF ONE HUNDRED DOLLARS ($100) OR THE AMOUNT YOU HAVE PAID US IN THE PAST TWELVE MONTHS. APPLICABLE LAW MAY NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY OR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. IN SUCH CASES, FACEBOOK'S LIABILITY WILL BE LIMITED TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW.

ANNEX 6 Facebook – Privacy Policy

FACEBOOK'S PRIVACY POLICY

http://www.facebook.com/note.php?note_id=10150162286770301

Date of Last Revision: April 22, 2010.

This policy contains eight sections, and you can jump to each by selecting the links below:

1. Introduction

TRUSTe Program. Facebook is a certified licensee of the TRUSTe Privacy Seal Program. This means that our privacy policy and practices have been reviewed by TRUSTe, an independent organization focused on reviewing privacy and security policies and practices, for compliance with its strict program requirements. This privacy policy covers the website www.facebook.com. The TRUSTe program covers only information that is collected through this Web site, and does not cover other information, such as information that may be collected through software downloaded from Facebook.

If you have any complaints about our policy or practices please let us know through this help page. If you are not satisfied with our response, you can contact TRUSTe.

2. Information We Receive

Information you provide to us:

Information About Yourself. When you sign up for Facebook you provide us with your name, email, gender, and birth date. During the registration process we give you the opportunity to connect with your friends, schools, and employers. You will also be able to add a picture of yourself. In some cases we may ask for additional information for security reasons or to provide specific services to you. Once you register you can provide other information about yourself by connecting with, for example, your current city, hometown, family, relationships, networks, activities, interests, and places. You can also provide personal information about yourself, such as your political and religious views.

Content. One of the primary reasons people use Facebook is to share content with others. Examples include when you update your status, upload or take a photo, upload or record a video, share a link, create an event or a group, make a comment, write something on someone's Wall, write a note, or send someone a message. If you do not

want us to store metadata associated with content you share on Facebook (such as photos), please remove the metadata before uploading the content.

Information we collect when you interact with Facebook:

Site activity information. We keep track of some of the actions you take on Facebook, such as adding connections (including joining a group or adding a friend), creating a photo album, sending a gift, poking another user, indicating you "like" a post, attending an event, or connecting with an application. In some cases you are also taking an action when you provide information or content to us. For example, if you share a video, in addition to storing the actual content you uploaded, we might log the fact that you shared it.

Information we receive from third parties:

Facebook Platform. We do not own or operate the applications or websites that you use through Facebook Platform (such as games and utilities). Whenever you connect with a Platform application or website, we will receive information from them, including information about actions you take. In some cases, in order to personalize the process of connecting, we may receive a limited amount of information even before you connect with the application or website.

Information from other websites. We may institute programs with advertising partners and other websites in which they share information with us:

- We may ask advertisers to tell us how our users responded to the ads we showed them (and for comparison purposes, how other users who didn't see the ads acted on their site). This data sharing, commonly known as "conversion tracking," helps us measure our advertising effectiveness and improve the quality of the advertisements you see.
- We may receive information about whether or not you've seen or interacted with certain ads on other sites in order to measure the effectiveness of those ads.

If in any of these cases we receive data that we do not already have, we will "anonymize" it within 180 days, meaning we will stop associating the information with any particular user. If we institute these programs, we will only use the information in the ways we explain in the "How We Use Your Information" section below.

Information from other users. We may collect information about you from other Facebook users, such as when a friend tags you in a photo, video, or place, provides friend details, or indicates a relationship with you.

3. Sharing information on Facebook.

This section explains how your privacy settings work, and how your information is shared on Facebook. You should always consider your privacy settings before sharing information on Facebook.

Name and Profile Picture. Facebook is designed to make it easy for you to find and connect with others. For this reason, your name and profile picture do not have privacy settings. If you are uncomfortable with sharing your profile picture, you should delete it (or not add one). You can also control who can find you when searching on Facebook or on public search engines using your search settings.

Contact Information. Your contact information settings control who can contact you on Facebook, and who can see your contact information such as your email and phone number(s). Remember that none of this information is required except for your email address, and you do not have to share your email address with anyone.

Personal Information. Your personal information settings control who can see your personal information, such as your religious and political views, if you choose to add them. We recommend that you share this information using the friends of friends setting.

Posts by Me. You can select a privacy setting for every post you make using the publisher on our site. Whether you are uploading a photo or posting a status update, you can control exactly who can see it at the time you create it. Whenever you share something look for the lock icon. Clicking on the lock will bring up a menu that lets you choose who will be able to see your post. If you decide not to select your setting at the time you post the content, your content will be shared consistent with your Posts by Me privacy setting.

Connections. Facebook enables you to connect with virtually anyone or anything you want, from your friends and family to the city you live in to the restaurants you like to visit to the bands and movies you love. Because it takes two to connect, your privacy settings only control who can see the connection on your profile page. If you are uncomfortable with the connection being publicly available, you should consider removing (or not making) the connection.

Gender and Birth Date. In addition to name and email address, we require you to provide your gender and birth date during the registration process. We ask for your date of birth to verify that you are 13 or older, and so that we can better limit your access to content and advertisements that are not age appropriate. Because your date of birth and gender are required, you cannot delete them. You can, however, edit your profile to hide all (or part) of such fields from other users.

Other. Here are some other things to remember:

- Some of the content you share and the actions you take will show up on your friends' home pages and other pages they visit.
- If another user tags you in a photo or video or at a place, you can remove the tag. You can also limit who can see that you have been tagged on your profile from your privacy settings.
- Even after you remove information from your profile or delete your account, copies of that information may remain viewable elsewhere to the extent it has been shared with others, it was otherwise distributed pursuant to your privacy settings, or it was copied or stored by other users.
- You understand that information might be reshared or copied by other users.
- Certain types of communications that you send to other users cannot be removed, such as messages.
- When you post information on another user's profile or comment on another user's post, that information will be subject to the other user's privacy settings.
- If you use an external source to publish information to Facebook (such as a mobile application or a Connect site), you should check the privacy setting for that post, as it is set by that external source.

"Everyone" Information. Information set to "everyone" is publicly available information, just like your name, profile picture, and connections. Such information may, for example, be accessed by everyone on the Internet (including people not logged into Facebook), be indexed by third party search engines, and be imported, exported, distributed, and redistributed by us and others without privacy limitations. Such information may also be associated with you, including your name and profile picture, even outside of Facebook, such as on public search engines and when you visit other sites on the internet. The default privacy setting for certain types of information you post on Facebook is set to "everyone." You can review and change the default settings in your privacy settings. If you delete "everyone" content that you posted on Facebook, we will remove it from your Facebook profile, but have no control over its use outside of Facebook.

4. Information You Share With Third Parties.

Facebook Platform. As mentioned above, we do not own or operate the applications or websites that use Facebook Platform. That means that when you use those applications and websites you are making your Facebook information available to someone other than Facebook. Prior to allowing them to access any information about you, we require them to agree to terms that limit their use of your information (which you can read about in Section 9 of our Statement of Rights and Responsibilities) and we use technical measures to ensure that they only obtain authorized information. To learn more about Platform, visit our About Platform page.

Connecting with an Application or Website. When you connect with an application or website it will have access to General Information about you. The term General Information includes your and your friends' names, profile pictures, gender, user IDs, connections, and any content shared using the Everyone privacy setting. We may also make information about the location of your computer or access device and your age available to applications and websites in order to help them implement appropriate security measures and control the distribution of age-appropriate content. If the application or website wants to access any other data, it will have to ask for your permission.

We give you tools to control how your information is shared with applications and websites that use Platform. For example, you can block specific applications from accessing your information by visiting your application settings or the application's "About" page. You can also use your privacy settings to limit which of your information is available to "everyone".

You should always review the policies of third party applications and websites to make sure you are comfortable with the ways in which they use information you share with them. We do not guarantee that they will follow our rules. If you find an application or website that violates our rules, you should report the violation to us on this help page and we will take action as necessary.

When your friends use Platform. If your friend connects with an application or website, it will be able to access your name, profile picture, gender, user ID, and information you have shared with "everyone." It will also be able to access your connections, except it will not be able to access your friend list. If you have already connected with (or have a separate account with) that website or application, it may also be able to connect you with your friend on that application or website. If the application or website wants to access any of your other content or information (including your friend list), it will have to

obtain specific permission from your friend. If your friend grants specific permission to the application or website, it will generally only be able to access content and information about you that your friend can access. In addition, it will only be allowed to use that content and information in connection with that friend. For example, if a friend gives an application access to a photo you only shared with your friends, that application could allow your friend to view or print the photo, but it cannot show that photo to anyone else.

We provide you with a number of tools to control how your information is shared when your friend connects with an application or website. For example, you can use your application privacy settings to limit some of the information your friends can make available to applications and websites. You can also block particular applications or websites from accessing your information. You can use your privacy settings to limit which friends can access your information, or limit which of your information is available to "everyone." You can also disconnect from a friend if you are uncomfortable with how they are using your information.

Pre-Approved Third-Party Websites and Applications. In order to provide you with useful social experiences off of Facebook, we occasionally need to provide General Information about you to pre-approved third party websites and applications that use Platform at the time you visit them (if you are still logged in to Facebook). Similarly, when one of your friends visits a pre-approved website or application, it will receive General Information about you so you and your friend can be connected on that website as well (if you also have an account with that website). In these cases we require these websites and applications to go through an approval process, and to enter into separate agreements designed to protect your privacy. For example, these agreements include provisions relating to the access and deletion of your General Information, along with your ability to opt-out of the experience being offered. You can also remove any pre-approved website or application you have visited here [add link], or block all pre-approved websites and applications from getting your General Information when you visit them here [add link]. In addition, if you log out of Facebook before visiting a pre-approved application or website, it will not be able to access your information. You can see a complete list of pre-approved websites on our About Platform page.

Advertisements. Sometimes the advertisers who present ads on Facebook use technological methods to measure the effectiveness of their ads and to personalize advertising content. You may opt-out of the placement of cookies by many of these advertisers here. You may also use your browser cookie settings to limit or prevent the placement of cookies by advertising networks.

Links. When you click on links on Facebook you may leave our site. We are not responsible for the privacy practices of other sites, and we encourage you to read their privacy statements.

5. How We Use Your Information

We use the information we collect to try to provide a safe, efficient, and customized experience. Here are some of the details on how we do that:

To manage the service. We use the information we collect to provide our services and features to you, to measure and improve those services and features, and to provide you with customer support. We use the information to prevent potentially illegal activities, and to enforce our Statement of Rights and Responsibilities. We also use a variety of

technological systems to detect and address anomalous activity and screen content to prevent abuse such as spam. These efforts may on occasion result in a temporary or permanent suspension or termination of some functions for some users.

To contact you. We may contact you with service-related announcements from time to time. You may opt out of all communications except essential updates on your account notifications page. We may include content you see on Facebook in the emails we send to you.

To serve personalized advertising to you. We don't share your information with advertisers without your consent. (An example of consent would be if you asked us to provide your shipping address to an advertiser to receive a free sample.) We allow advertisers to choose the characteristics of users who will see their advertisements and we may use any of the non-personally identifiable attributes we have collected (including information you may have decided not to show to other users, such as your birth year or other sensitive personal information or preferences) to select the appropriate audience for those advertisements. For example, we might use your interest in soccer to show you ads for soccer equipment, but we do not tell the soccer equipment company who you are. You can see the criteria advertisers may select by visiting our advertising page. Even though we do not share your information with advertisers without your consent, when you click on or otherwise interact with an advertisement there is a possibility that the advertiser may place a cookie in your browser and note that it meets the criteria they selected.

To supplement your profile. We may use information about you that we collect from other Facebook users to supplement your profile (such as when you are tagged in a photo or mentioned in a status update). In such cases we generally give you the ability to remove the content (such as allowing you to remove a photo tag of you) or limit its visibility on your profile.

To make suggestions. We use your profile information, the addresses you import through our contact importers, and other relevant information, to help you connect with your friends, including making suggestions to you and other users that you connect with on Facebook. For example, if another user imports the same email address as you do, we may suggest that you connect with each other. If you want to limit your visibility in suggestions we make to other people, you can adjust your search visibility privacy setting, as you will only be visible in our suggestions to the extent you choose to be visible in public search listings. You may also block specific individual users from being suggested to you and you from being suggested to them.

To help your friends find you. We allow other users to use contact information they have about you, such as your email address, to find you, including through contact importers and search. You can prevent other users from using your email address to find you using your search setting.

6. How We Share Information

Facebook is about sharing information with others — friends and people in your communities — while providing you with privacy settings that you can use to restrict other users from accessing some of your information. We share your information with third parties when we believe the sharing is permitted by you, reasonably necessary to offer our services, or when legally required to do so. For example:

When you invite a friend to join. When you ask us to invite a friend to join Facebook, we will send your friend a message on your behalf using your name. The invitation may also contain information about other users your friend might know. We may also send up to two reminders to them in your name. You can see who has accepted your invitations, send reminders, and delete your friends' email addresses on your invite history page. If your friend does not want us to keep their information, we will also remove it at their request by using this help page.

When you choose to share your information with marketers. You may choose to share information with marketers or electronic commerce providers that are not associated with Facebook through on-site offers. This is entirely at your discretion and we will not provide your information to these marketers without your consent.

To help your friends find you. By default, we make certain information you have posted to your profile available in search results on Facebook to help your friends find you. However, you can control who can see some of this information, as well as who can find you in searches, through your privacy settings. We also partner with email and instant messaging providers to help their users identify which of their contacts are Facebook users, so that we can promote Facebook to those users.

To give search engines access to publicly available information. We generally limit search engines' access to our site. We may allow them to access information set to the "everyone" setting (along with your name and profile picture) and your profile information that is visible to everyone. You can change the visibility of some of your profile information using your privacy settings. You can also prevent search engines from indexing your profile using your search settings.

To help improve or promote our service. Sometimes we share aggregated information with third parties to help improve or promote our service. But we only do so in such a way that no individual user can be identified or linked to any specific action or information.

To provide you with services. We may provide information to service providers that help us bring you the services we offer. For example, we may use third parties to help host our website, send out email updates about Facebook, remove repetitive information from our user lists, process payments, or provide search results or links (including sponsored links). These service providers may have access to your personal information for use for a limited time, but when this occurs we implement reasonable contractual and technical protections to limit their use of that information to helping us provide the service.

To advertise our services. We may ask advertisers outside of Facebook to display ads promoting our services. We may ask them to deliver those ads based on the presence of a cookie, but in doing so will not share any other information with the advertiser.

To offer joint services. We may provide services jointly with other companies, such as the classifieds service in the Facebook Marketplace. If you use these services, we may share your information to facilitate that service. However, we will identify the partner and present the joint service provider's privacy policy to you before you use that service.

To respond to legal requests and prevent harm. We may disclose information pursuant to subpoenas, court orders, or other requests (including criminal and civil matters) if we have a good faith belief that the response is required by law. This may include respecting requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law under the local laws in that jurisdiction, apply to users from that jurisdiction, and are consistent with generally accepted international standards. We may also share information when we have a good faith belief it is necessary to prevent fraud or other illegal activity, to prevent imminent bodily harm, or to protect ourselves and you from people violating our Statement of Rights and Responsibilities. This may include sharing information with other companies, lawyers, courts or other government entities.

Transfer in the Event of Sale or Change of Control. If the ownership of all or substantially all of our business changes, we may transfer your information to the new owner so that the service can continue to operate. In such a case, your information would remain subject to the promises made in any pre-existing Privacy Policy.

8. How We Protect Information

We do our best to keep your information secure, but we need your help. For more detailed information about staying safe on Facebook, visit the Facebook Security Page.

Steps we take to keep your information secure. We keep your account information on a secured server behind a firewall. When you enter sensitive information (such as credit card numbers and passwords), we encrypt that information using secure socket layer technology (SSL). We also use automated and social measures to enhance security, such as analyzing account behavior for fraudulent or otherwise anomalous behavior, may limit use of site features in response to possible signs of abuse, may remove inappropriate content or links to illegal content, and may suspend or disable accounts for violations of our Statement of Rights and Responsibilities.

Risks inherent in sharing information. Although we allow you to set privacy options that limit access to your information, please be aware that no security measures are perfect or impenetrable. We cannot control the actions of other users with whom you share your information. We cannot guarantee that only authorized persons will view your information. We cannot ensure that information you share on Facebook will not become publicly available. We are not responsible for third party circumvention of any privacy settings or security measures on Facebook. You can reduce these risks by using common sense security practices such as choosing a strong password, using different passwords for different services, and using up to date antivirus software.

Report Violations. You should report any security violations to us on this help page.

ANNEX 7 Google – Terms of Service

GOOGLE TERMS OF SERVICE

http://www.google.com/accounts/TOS

3. Language of the Terms

3.1 Where Google has provided you with a translation of the English language version of the Terms, then you agree that the translation is provided for your convenience only and that the English language versions of the Terms will govern your relationship with Google.

3.2 If there is any contradiction between what the English language version of the Terms says and what a translation says, then the English language version shall take precedence.

7. Privacy and your personal information

7.1 For information about Google's data protection practices, please read Google's privacy policy at http://www.google.com/privacy.html. This policy explains how Google treats your personal information, and protects your privacy, when you use the Services.

7.2 You agree to the use of your data in accordance with Google's privacy policies.

9. Proprietary rights

9.4 Other than the limited license set forth in Section 11, Google acknowledges and agrees that it obtains no right, title or interest from you (or your licensors) under these Terms in or to any Content that you submit, post, transmit or display on, or through, the Services, including any intellectual property rights which subsist in that Content (whether those rights happen to be registered or not, and wherever in the world those rights may exist). Unless you have agreed otherwise in writing with Google, you agree that you are responsible for protecting and enforcing those rights and that Google has no obligation to do so on your behalf.

9.5 You agree that you shall not remove, obscure, or alter any proprietary rights notices (including copyright and trade mark notices) which may be affixed to or contained within the Services.

9.6 Unless you have been expressly authorized to do so in writing by Google, you agree that in using the Services, you will not use any trade mark, service mark, trade name, logo of any company or organization in a way that is likely or intended to cause confusion about the owner or authorized user of such marks, names or logos.

11. Content license from you

11.1 You retain copyright and any other rights you already hold in Content which you submit, post or display on or through, the Services. By submitting, posting or displaying the content you give Google a perpetual, irrevocable, worldwide, royalty-free, and non-exclusive license to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute any Content which you submit, post or display on or through, the Services. This license is for the sole purpose of enabling Google to display, distribute and promote the Services and may be revoked for certain Services as defined in the Additional Terms of those Services.

11.2 You agree that this license includes a right for Google to make such Content available to other companies, organizations or individuals with whom Google has relationships for the provision of syndicated services, and to use such Content in connection with the provision of those services.

11.3 You understand that Google, in performing the required technical steps to provide the Services to our users, may (a) transmit or distribute your Content over various public networks and in various media; and (b) make such changes to your Content as are necessary to conform and adapt that Content to the technical requirements of connecting networks, devices, services or media. You agree that this license shall permit Google to take these actions.

11.4 You confirm and warrant to Google that you have all the rights, power and authority necessary to grant the above license.

14. EXCLUSION OF WARRANTIES

14.1 NOTHING IN THESE TERMS, INCLUDING SECTIONS 14 AND 15, SHALL EXCLUDE OR LIMIT GOOGLE'S WARRANTY OR LIABILITY FOR LOSSES WHICH MAY NOT BE LAWFULLY EXCLUDED OR LIMITED BY APPLICABLE LAW. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES OR CONDITIONS OR THE LIMITATION OR EXCLUSION OF LIABILITY FOR LOSS OR DAMAGE CAUSED BY NEGLIGENCE, BREACH OF CONTRACT OR BREACH OF IMPLIED TERMS, OR INCIDENTAL OR CONSEQUENTIAL DAMAGES. ACCORDINGLY, ONLY THE LIMITATIONS WHICH ARE LAWFUL IN YOUR JURISDICTION WILL APPLY TO YOU AND OUR LIABILITY WILL BE LIMITED TO THE MAXIMUM EXTENT PERMITTED BY LAW.

14.2 YOU EXPRESSLY UNDERSTAND AND AGREE THAT YOUR USE OF THE SERVICES IS AT YOUR SOLE RISK AND THAT THE SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE."

14.3 IN PARTICULAR, GOOGLE, ITS SUBSIDIARIES AND AFFILIATES, AND ITS LICENSORS DO NOT REPRESENT OR WARRANT TO YOU THAT:

(A) YOUR USE OF THE SERVICES WILL MEET YOUR REQUIREMENTS,

(B) YOUR USE OF THE SERVICES WILL BE UNINTERRUPTED, TIMELY, SECURE OR FREE FROM ERROR,

(C) ANY INFORMATION OBTAINED BY YOU AS A RESULT OF YOUR USE OF THE SERVICES WILL BE ACCURATE OR RELIABLE, AND

(D) THAT DEFECTS IN THE OPERATION OR FUNCTIONALITY OF ANY SOFTWARE PROVIDED TO YOU AS PART OF THE SERVICES WILL BE CORRECTED.

14.4 ANY MATERIAL DOWNLOADED OR OTHERWISE OBTAINED THROUGH THE USE OF THE SERVICES IS DONE AT YOUR OWN DISCRETION AND RISK AND THAT YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE TO YOUR COMPUTER SYSTEM OR OTHER DEVICE OR LOSS OF DATA THAT RESULTS FROM THE DOWNLOAD OF ANY SUCH MATERIAL.

14.5 NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED BY YOU FROM GOOGLE OR THROUGH OR FROM THE SERVICES SHALL CREATE ANY WARRANTY NOT EXPRESSLY STATED IN THE TERMS.

14.6 GOOGLE FURTHER EXPRESSLY DISCLAIMS ALL WARRANTIES AND CONDITIONS OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.

15. LIMITATION OF LIABILITY

15.1 SUBJECT TO OVERALL PROVISION IN PARAGRAPH 14.1 ABOVE, YOU EXPRESSLY UNDERSTAND AND AGREE THAT GOOGLE, ITS SUBSIDIARIES AND AFFILIATES, AND ITS LICENSORS SHALL NOT BE LIABLE TO YOU FOR:

(A) ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL CONSEQUENTIAL OR EXEMPLARY DAMAGES WHICH MAY BE INCURRED BY YOU, HOWEVER CAUSED AND UNDER ANY THEORY OF LIABILITY.. THIS SHALL INCLUDE, BUT NOT BE LIMITED TO, ANY LOSS OF PROFIT (WHETHER INCURRED DIRECTLY OR INDIRECTLY), ANY LOSS OF GOODWILL OR BUSINESS REPUTATION, ANY LOSS OF DATA SUFFERED, COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR OTHER INTANGIBLE LOSS;

(B) ANY LOSS OR DAMAGE WHICH MAY BE INCURRED BY YOU, INCLUDING BUT NOT LIMITED TO LOSS OR DAMAGE AS A RESULT OF:

(I) ANY RELIANCE PLACED BY YOU ON THE COMPLETENESS, ACCURACY OR EXISTENCE OF ANY ADVERTISING, OR AS A RESULT OF ANY RELATIONSHIP OR TRANSACTION BETWEEN YOU AND ANY ADVERTISER OR SPONSOR WHOSE ADVERTISING APPEARS ON THE SERVICES;

(II) ANY CHANGES WHICH GOOGLE MAY MAKE TO THE SERVICES, OR FOR ANY PERMANENT OR TEMPORARY CESSATION IN THE PROVISION OF THE SERVICES (OR ANY FEATURES WITHIN THE SERVICES);

(III) THE DELETION OF, CORRUPTION OF, OR FAILURE TO STORE, ANY CONTENT AND OTHER COMMUNICATIONS DATA MAINTAINED OR TRANSMITTED BY OR THROUGH YOUR USE OF THE SERVICES;

(IV) YOUR FAILURE TO PROVIDE GOOGLE WITH ACCURATE ACCOUNT INFORMATION;

(V) YOUR FAILURE TO KEEP YOUR PASSWORD OR ACCOUNT DETAILS SECURE AND CONFIDENTIAL.

15.2 THE LIMITATIONS ON GOOGLE'S LIABILITY TO YOU IN PARAGRAPH 15.1 ABOVE SHALL APPLY WHETHER OR NOT GOOGLE HAS BEEN ADVISED OF OR SHOULD HAVE BEEN AWARE OF THE POSSIBILITY OF ANY SUCH LOSSES ARISING.

17. Advertisements

17.1 Some of the Services are supported by advertising revenue and may display advertisements and promotions. These advertisements may be targeted to the content of information stored on the Services, queries made through the Services or other information.

17.2 The manner, mode and extent of advertising by Google on the Services are subject to change without specific notice to you.

17.3 In consideration for Google granting you access to and use of the Services, you agree that Google may place such advertising on the Services.

19. Changes to the Terms

19.1 Google may make changes to the Universal Terms or Additional Terms from time to time. When these changes are made, Google will make a new copy of the Universal Terms available at http://www.google.com/accounts/TOS?hl=en and any new Additional Terms will be made available to you from within, or through, the affected Services.

19.2 You understand and agree that if you use the Services after the date on which the Universal Terms or Additional Terms have changed, Google will treat your use as acceptance of the updated Universal Terms or Additional Terms.

20. General legal terms

20.7 The Terms, and your relationship with Google under the Terms, shall be governed by the laws of the State of California without regard to its conflict of laws provisions. You and Google agree to submit to the exclusive jurisdiction of the courts located within the county of Santa Clara, California to resolve any legal matter arising from the Terms. Notwithstanding this, you agree that Google shall still be allowed to apply for injunctive remedies (or an equivalent type of urgent legal relief) in any jurisdiction.

April 16, 2007

ANNEX 8 Google – Additional Clauses

Additional Terms of Service

http://www.google.com/google-d-s/intl/fr/addlterms.html

Thank you for using Google Docs! By using Google Docs (the "Service"), you accept and agree to be bound by the Google Terms of Service, the Google Docs Program Policies, the Google Docs Privacy Policy, the Google Docs Copyright Notices, as well as these additional terms and conditions (collectively the "Terms of Service"). It is important for you to read each of these documents, as they form a legal agreement between you and Google regarding your use of the Service.

Privacy and your personal information

Section 7 of the Google Terms of Service governing Google Docs is replaced in its entirety by:

7.1 For information about Google's data protection practices, please read the Google Docs Privacy Policy at http://www.google.com/google-d-s/intl/en/privacy.html. This policy explains how Google treats your personal information, and protects your privacy, when you use the Service.

7.2 You agree to the use of your data in accordance with Google's privacy policies.

Content License from You

Section 11 of the Google Terms of Service governing Google Docs is replaced in its entirety by:

11.1 You retain copyright and any other rights you already hold in Content which you submit, share, upload, post or display on or through, the Service. By submitting, sharing, uploading, posting or displaying the Content you give Google a worldwide, royalty-free, and non-exclusive license to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute any Content which you submit, share, upload, post or display on or through the Service for the sole purpose of enabling Google to provide you with the Service in accordance with the Google Docs Privacy Policy.

11.2 You understand that Google, in performing the required technical steps to provide the Service to our users, may (a) transmit or distribute your Content over various public networks and in various media; and (b) make such changes to your Content as are necessary to conform and adapt that Content to the technical requirements of connecting networks, devices, services or media. You agree that this license shall permit Google to take these actions.

11.3 You confirm and warrant to Google that you have all the rights, power and authority necessary to grant the above license. You agree that you will not submit, share, upload, post or display Content on or through, the Service that is copyrighted, protected by trade secret or otherwise subject to third party proprietary rights, including privacy and publicity rights, unless you are the owner of such rights or have permission from their rightful owner to submit, share, upload, post or display the Content and to grant Google all of the license rights granted in this Section.

Appropriate Conduct
You agree that you are responsible for your own conduct and Content while using the Service and for any consequences thereof. You agree to use the Service only for purposes that are legal, proper and in accordance with these Terms of Service.

Copyright and Account Termination Policy
Google does not permit infringement of intellectual property rights on its Services. Google will remove Content if properly notified in accordance with Google's DMCA process (http://www.google.com/dmca.html) that such Content infringes on another's copyright. Without prior notice and at any time at its sole discretion, Google reserves the right to remove any Content, disable your ability to share or upload Content within the Service, or terminate your access to the Service (a) for uploading or sharing such Content in violation of these Terms of Service; or (b) if, under appropriate circumstances, you are determined to be a repeat infringer.

Google reserves the right in its sole discretion to decide whether your conduct is inappropriate and whether it complies with these Terms of Service for violations other than copyright infringement, such as, but not limited to, pornography, obscene or defamatory material, or excessive length. Google may terminate your access for such inappropriate conduct in violation of these Terms of Service at any time and remove any such objectionable Content, without prior notice and at its sole discretion.

Your Use of Template Features
This version of Google Docs may contain pre-written templates.

These templates were created by Google or by third parties. As between you and the creators of the templates, any intellectual property or proprietary rights remain with the creators.

These templates, and the information contained in them: (a) are meant to serve as suggestions only; and (b) are not a substitute for professional advice or specific, authoritative knowledge or direction.

Google does not promise that the templates will work for your purposes, or that they are free from viruses, bugs, or other defects. The templates are provided "as is" and without warranty of any kind. You alone bear the risk of using them. Google and its suppliers provide no express warranties, guarantees and conditions with regard to the templates. To the extent permitted under applicable law, Google excludes the implied warranties and conditions of merchantability, fitness for a particular purpose, workmanlike effort, title and non-infringement.

Submission of Templates
If you choose to submit your template through Google Docs, you direct and authorize Google and its affiliates to host, link to, and otherwise incorporate your template into Google Docs, and you grant Google and its end users a worldwide, royalty-free, non-exclusive license to exercise the rights in the template, as stated below:

- to reproduce the template;
- to create and reproduce derivative works of the template;
- to display publicly and distribute copies of the template;
- to display publicly and distribute copies of derivative works of the template.

You agree that your license to Google end users will be perpetual. Furthermore, for the avoidance of doubt, Google reserves, and you grant Google, the right to syndicate the template submitted by you through Google Docs and use that template in connection with any of the

Services offered by Google. You retain the right to stop distributing the template through the Google Docs template gallery at any time; provided, however that any such election will not serve to withdraw the licenses granted to Google end users under these Terms of Service. In order to stop distributing the template through the Google Docs template gallery, you must utilize the template removal function provided within the Service, in which case the template removal will be effective within a reasonable amount of time.

You represent and warrant that (a) you own or have obtained the necessary legal rights to provide all templates you submit through Google Docs, and will maintain these rights for as long as the template is available to Google end users; and (b) all of the templates you submit through Google Docs abide by the posted Program Policies.

Google claims no ownership over any templates you submit through Google Docs. You retain copyright and any other rights, including all intellectual property rights, you already hold in the templates. You agree that you are responsible for protecting and enforcing those rights and that Google has no obligation to do so on your behalf.

You agree that you are solely responsible for (and that Google has no responsibility to you or to any third party for) any template that you submit. Google is not in any way responsible for the subsequent use or misuse by Google end users who access your template.

Indemnity

You hereby agree to indemnify, defend and hold Google, its partners, officers, directors, agents, affiliates, and licensors ("**the Indemnified Parties**") harmless from and against any claim or liability arising out of (a) any Content you submit, share, upload, post or display on or to the Service; (b) any use by Google end users of your Content; (c) any breach of or noncompliance with any representation, warranty or obligation in these Terms or applicable policies; and (d) any claim that your Content violates any applicable law, including without limitation that it infringes the rights of a third party. You shall cooperate fully in the defense of any claim. Google reserves the right, at its own expense, to assume the exclusive defense and control of any matter subject to indemnification by you. You acknowledge that damages for improper use of Google Docs may be irreparable; therefore, Google is entitled to seek equitable relief, including injunction and preliminary injunction, in addition to all other remedies. This section shall take precedence only over the indemnity provision provided in any Additional Terms as it relates to Google Docs, and not to any other Services.

ANNEX 9 Google – Privacy Policy

GOOGLE DOCUMENTS PRIVACY POLICY

Note: We were unable to find an archived version of the english version of this document (http://www.google.com/google-d-s/intl/en/privacy.html). We reproduce below the french version.

30 octobre 2009
Les règles de confidentialité de Google définissent la manière dont nous traitons vos informations personnelles lorsque vous faites usage des services Google, y compris les informations transmises à Google Documents. Vous trouverez ci-dessous les règles de confidentialité propres à Google Documents.
http://www.google.com/google-d-s/intl/fr/privacy.html

Informations personnelles

- *Activité du compte.* Pour créer des fichiers dans Google Documents, vous devez disposer d'un compte Google. Lorsque vous créez votre compte, Google vous demande des informations personnelles, notamment votre adresse e-mail et un mot de passe, afin de protéger votre compte contre tout accès non autorisé. Les serveurs de Google enregistrent automatiquement certaines informations sur l'usage que vous faites du service Google Documents. Comme pour les autres services Web, Google enregistre des informations telles que l'activité du compte (par exemple, l'utilisation de la zone de stockage allouée, le nombre de connexions, les actions exécutées), les données affichées ou sur lesquelles l'utilisateur a cliqué (par exemple, les éléments de l'interface utilisateur et les liens) et d'autres informations de connexion (par exemple, le type de navigateur, l'adresse IP, la date et l'heure d'accès, l'identifiant de cookie et l'URL précédemment visitée).
- *Contenu.* Afin que nous puissions vous fournir le service proposé, Google Documents doit enregistrer, traiter et conserver vos fichiers (ainsi que les versions précédentes de ces fichiers), vos listes de partage et toute autre donnée associée à votre compte.

Utilisations

- Nous utilisons ces informations en interne en vue de vous offrir un service optimal, notamment pour améliorer l'interface utilisateur de Google Documents et assurer un service cohérent et fiable.
- Si vous le souhaitez, les fichiers que vous créez, importez ou copiez sur Google Documents peuvent être lus, copiés, utilisés et redistribués par des personnes que vous connaissez ou que vous ne connaissez pas (selon votre choix). Les informations que vous communiquez par le biais de la fonction de chat de Google Documents peuvent être lues, copiées, utilisées et redistribuées par les personnes participant au chat. Faites par conséquent preuve de prudence lorsque vous fournissez des informations personnelles sensibles (numéro de sécurité sociale, informations financières ou adresse et numéro de téléphone personnels) dans les fichiers que vous partagez ou au cours des sessions de chat.
- Certaines fonctionnalités (les gadgets par exemple) sont fournies par des tiers, qui peuvent recevoir et traiter vos données. En utilisant l'une de ces fonctionnalités, vous

acceptez de partager des données avec ce tiers, et vous l'autorisez à les traiter. Les présentes règles de confidentialité ne régissent pas l'accès à vos données par ces tiers.

Vos choix

- Vous pouvez mettre fin à votre utilisation de Google Documents à tout moment.
- Vous pouvez supprimer définitivement tout fichier créé dans Google Documents. En raison du mode de maintenance de ce service, il faut parfois attendre jusqu'à 30 jours avant que les copies résiduelles de vos fichiers ne soient supprimées de nos serveurs actifs. Ces copies peuvent également être conservées sur nos systèmes de sauvegarde hors ligne pendant 60 jours supplémentaires.

Autres informations

Google respecte les principes de confidentialité de la "Sphère de sécurité" (Safe Harbor) des United States. Pour plus d'informations sur le cadre de ces dispositions ou sur notre adhésion, consultez le site Web du Ministère du Commerce des United States.

Vous trouverez des informations supplémentaires sur Google Documents ici.

Pour plus d'informations sur notre politique en matière de respect de la vie privée, consultez nos règles de confidentialité. Pour toute question relative au produit ou à votre compte, consultez la page Aide Google.

ANNEX 10 Microsoft – Services Agreement

MICROSOFT SERVICES AGREEMENT

http://explore.live.com/microsoft-service-agreement?ref=none

About Bing data suppliers
Code of conduct
Microsoft Services Agreement

Updated August 1, 2010
Effective August 31, 2010

Thank you for choosing Microsoft!

1. What the contract covers

This is a contract between you and the Microsoft company listed in Section 13 ("Microsoft," "we," "us," or "our") for use of the service that Microsoft supplies. Sections 1–13 apply across the service. Sections 14 and 15 apply only if the service involves payments to or from Microsoft. Sections 16–20 apply only if you use the software or services identified in those sections. Some of these services may not be fully available in your country or region.

Please note that we don't provide additional warranties for the service. This contract also limits our liability to you. See Sections 9 and 10 for details.

5. Your content

Except for material that we license to you, we don't claim ownership of the content you provide on the service. Your content remains your content. We also don't control, verify, or endorse the content that you and others make available on the service.

You control who may access your content. If you share content in public areas of the service or in shared areas available to others you've chosen, then you agree that anyone you've shared content with may use that content. When you give others access to your content on the service, you grant them free, nonexclusive permission to use, reproduce, distribute, display, transmit, and communicate to the public the content solely in connection with the service and other products and services made available by Microsoft. If you don't want others to have those rights, don't use the service to share your content.

You understand that Microsoft may need, and you hereby grant Microsoft the right, to use, modify, adapt, reproduce, distribute, and display content posted on the service solely to the extent necessary to provide the service.

Please respect the rights of artists, inventors, and creators. Content may be protected by copyright. People appearing in content may have a right to control the use of their image. If you share content on the service in a way that infringes others' copyrights, other intellectual property rights, or privacy rights, you're breaching this contract. You

represent and warrant that you have all the rights necessary for you to grant the rights in this section and the use of the content doesn't violate any law. We won't pay you for your content. We may refuse to publish your content for any or no reason. We may remove your content from the service at any time if you breach this contract or if we cancel or suspend the service.

You're responsible for backing up the data that you store on the service. If your service is suspended or canceled, we may permanently delete your data from our servers. We have no obligation to return data to you after the service is suspended or canceled. If data is stored with an expiration date, we may also delete the data as of that date. Data that is deleted may be irretrievable.

6. Privacy

In order to operate and provide the service, we collect certain information about you. As part of the service, we may also automatically upload information about your computer, your use of the service, and service performance. We use and protect that information as described in the Microsoft Online Privacy Statement (http://go.microsoft.com/fwlink/?LinkId=74170). In particular, we may access or disclose information about you, including the content of your communications, in order to: (a) comply with the law or respond to lawful requests or legal process; (b) protect the rights or property of Microsoft or our customers, including the enforcement of our agreements or policies governing your use of the service; or (c) act on a good faith belief that such access or disclosure is necessary to protect the personal safety of Microsoft employees, customers, or the public.

The service is a private computer network that Microsoft operates for the benefit of itself and its customers. Microsoft retains the right to block or otherwise prevent delivery of any type of email or other communication to or from the service as part of our efforts to protect the service, protect our customers, or stop you from breaching this contract. The technology or other means we use may hinder or break your use of the service.

8. How we may change the contract

If we amend this contract, then we'll notify you before the change takes effect. We may give this notice by posting it on the service or by any other reasonable means. If you don't agree to the change, we're not obligated to keep providing the service, and you must cancel and stop using the service before the change becomes effective. Otherwise, the new terms will apply to you.

9. NO WARRANTY

We provide the service "as is," "with all faults," and "as available." We don't guarantee the accuracy or timeliness of information available from the service. You acknowledge that computer and telecommunications systems are not fault-free and occasional periods of downtime occur. We do not guarantee the service will be uninterrupted, timely, secure, or error-free, or that data loss will not occur. We and our affiliates, resellers, distributors, and vendors give no express warranties, guarantees, or conditions. We exclude any implied warranties, including for merchantability, satisfactory quality, fitness for a particular purpose, workmanlike effort, and noninfringement. You may have certain rights under your local law. Nothing in this contract is intended to affect those rights, if they are applicable.

10. LIABILITY LIMITATION

You can recover from Microsoft and our affiliates, resellers, distributors, and vendors only direct damages up to an amount equal to your service fee for one month. You cannot recover any other damages, including consequential, lost profits, special, indirect, incidental, or punitive damages.

The limitations and exclusions apply to anything related to this contract, for example:

- The service.
- Loss of data.
- Content (including code) on third-party websites, third-party programs, or third-party conduct accessed via the service.
- Viruses or other disabling features that affect your access to or use of the service.
- Incompatibility between the service and other services, software, and hardware.
- Delays or failures you may have in starting or completing transmissions or transactions in connection with the service in an accurate or timely manner.
- Claims for breach of contract; breach of warranty, guarantee or condition; strict liability; tort (including negligence or breach of statutory duty); or misrepresentation.

The limitations and exclusions also apply if this remedy does not fully compensate you for any losses or fails of its essential purpose or if we knew or should have known about the possibility of the damages.

Some or all of these limitations or exclusions may not apply to you if your state, province, or country does not allow the exclusion or limitation of incidental, consequential, or other damages.

11. Changes to the service and cancellation

We may change the service or delete features at any time for any reason. A particular service may be a prerelease version—a beta, for example—and may not work correctly or in the way a final version might work. We may significantly change the final version or decide not to release a final version.

We may cancel or suspend your service and your access to the Windows Live ID network at any time without notice and for any reason. Our reasons for cancellation may include that we stop providing the service in your region or that you breach this contract, fail to sign in to the Windows Live ID network during a 90-day period, or don't pay fees that you owe to us or to our agents. If your service is canceled, your right to use the service stops immediately. If we cancel your credentials, your right to use Windows Live ID stops immediately. Cancellation of the service or credentials won't alter your obligation to pay all charges made to your billing account. If we cancel the service in its entirety without cause, we'll refund to you on a pro-rata basis any payments that you have made based on the portion of your service that would otherwise remain.

You may cancel the service at any time and for any reason. If it's a paid service, some charges may apply. Sections 6, 9–13, 14 (for amounts incurred before termination), 15, and those that by their terms apply after termination of this contract will survive any termination of this contract.

13. Contracting party, choice of law and location for resolving disputes

- If you live in or your business is headquartered in North or South America, you're contracting with Microsoft Corp., One Microsoft Way, Redmond, WA 98052, USA, and Washington State law governs the interpretation of this contract and applies to claims for breach of it, regardless of conflict of laws principles. All other claims, including claims regarding consumer protection laws, unfair competition laws, and in tort, will be subject to the laws of your state of residence in the United States, or, if you live outside the United States, the laws of the country to which we direct your service. You and we irrevocably consent to the exclusive jurisdiction and venue of the state or federal courts in King County, Washington, USA, for all disputes arising out of or relating to this contract.
- If you live in or your business is headquartered in Europe, you're contracting with Microsoft Luxembourg S.à.r.l., 20 Rue Eugene Ruppert, Immeuble Laccolith, 1st Floor, L-2543 Luxembourg. All claims, including claims regarding consumer protection laws, unfair competition laws, and in tort, will be subject to the laws of Luxembourg or of the country in which you reside. With respect to jurisdiction, you may choose the responsible court in Luxembourg or in the country in which you reside for all disputes arising out of or relating to this contract.
- If you live in or your business is headquartered in the Middle East or Africa, you're contracting with Microsoft Luxembourg S.à.r.l., 20 Rue Eugene Ruppert, Immeuble Laccolith, 1st Floor, L-2543 Luxembourg, and the laws of Luxembourg govern the interpretation of this contract and apply to claims for breach of it, regardless of conflict of laws principles. All other claims, including claims regarding consumer protection laws, unfair competition laws, and in tort, will be subject to the laws of the country to which we direct your service. You and we irrevocably agree to the exclusive jurisdiction and venue of the Luxembourg courts for all disputes arising out of or relating to this contract.
- If you live in or your business is headquartered in Japan, you're contracting with Microsoft Japan Co. Ltd (MSKK), Shinagawa Grand Central Tower 2-16-3, Konan, Minato-ku, Tokyo 108-0075. The laws of Japan govern this contract and any matters arising out of or relating to it. You and we irrevocably agree to the exclusive original jurisdiction and venue of the Tokyo District Court for all disputes arising out of or relating to this contract.
- If you live in or your business is headquartered in Australia, Hong Kong, Indonesia, Malaysia, New Zealand, Philippines, Singapore, Thailand, or Vietnam, you're contracting with Microsoft Operations, Pte Ltd, 1 Marina Boulevard, #22-01, Singapore 01898, and the laws of Singapore govern this contract. Any dispute arising out of or in connection with this contract, including any question regarding its existence, validity, or termination, will be referred to and finally resolved by arbitration in Singapore in accordance with the Arbitration Rules of the Singapore International Arbitration Center (SIAC), which rules are deemed to be incorporated by reference into this clause. The Tribunal will consist of one arbitrator to be appointed by the Chairman of SIAC. The language of arbitration will be English. The decision of the arbitrator will be final, binding, and incontestable, and it may be used as a basis for judgment in any country or region.
- If you live in or your business is headquartered in India, you're contracting with Microsoft Regional Sales Corp., a corporation organized under the laws of the State of Nevada, USA, with a branch in Singapore, having its principal place of business at 438B Alexandra Road, #04-09/12, Block B, Alexandra Technopark, Singapore, 119968, and Washington State law governs this contract, regardless of conflict of laws principles. Any dispute arising out of or in connection with this contract,

including any question regarding its existence, validity, or termination, will be referred to and finally resolved by arbitration in Singapore in accordance with the Arbitration Rules of the Singapore International Arbitration Center (SIAC), which rules are deemed to be incorporated by reference into this clause. The Tribunal will consist of one arbitrator to be appointed by the Chairman of SIAC. The language of arbitration will be English. The decision of the arbitrator will be final, binding, and incontestable, and it may be used as a basis for judgment in India or elsewhere.

- If you live in or your business is headquartered in China, you're contracting with Shanghai MSN Network Communications Technology Company Limited, Suite B, 8th Floor, Building Ding, No. 555, Dongchuan Road, Minhang District, Shanghai, PRC, for your use of MSN, Bing, or Windows Live Messenger; PRC law governs this contract as it relates to your use of the services under this contract operated by Shanghai MSN Network Communications Technology Company Limited. For your use of MSN, Bing, or Windows Live Messenger under this contract, any dispute arising out of or in connection with this contract, including any question regarding the existence, validity, or termination of this contract, will be referred to and finally resolved by arbitration in Hong Kong under the auspices of the Hong Kong International Arbitration Centre ("HKIAC") in accordance with the UNCITRAL Arbitration Rules, which are deemed to be incorporated by reference into this clause. For such arbitration, there will be one arbitrator, who will be appointed by HKIAC in accordance with the UNCITRAL Arbitration Rules. The language of arbitration will be English. The decision of the arbitrator will be final, binding, and incontestable and may be used as a basis for judgment in China or elsewhere. For your use of all other services under this contract, you're contracting with Microsoft Corp., One Microsoft Way, Redmond, WA 98052, USA. As to those services, Washington State law governs this contract, regardless of conflict of laws principles. The jurisdiction of the state or federal courts in King County, Washington, USA, is nonexclusive.
- If you live in or your business is headquartered in Korea, you're contracting with Microsoft Korea, Inc., 6th Floor, POSCO Center, 892 Daechi-Dong, Kangnam-Gu, Seoul, 135-777, Korea, and the laws of the Republic of Korea govern this contract. You and we irrevocably agree to exclusive original jurisdiction and venue of the Seoul District Court for all disputes arising out of or relating to this contract.
- If you live in or your business is headquartered in Taiwan, you're contracting with Microsoft Taiwan Corp., 8F, No 7 Sungren Road, Shinyi Chiu, Taipei, Taiwan 110, and the laws of Taiwan govern this contract. You and we irrevocably designate the Taipei District Court as the court of first instance having jurisdiction over any disputes arising out of or in connection with this contract.

ANNEX 11 Microsoft – Online Policy Statement

MICROSOFT ONLINE PRIVACY STATEMENT

(last updated April 2012)

http://privacy.microsoft.com/en-ca/fullnotice.mspx

Microsoft is committed to protecting the confidentiality of your data. Please read the Microsoft Online Privacy Statement below and also any supplemental information listed to the right for further details about particular Microsoft sites and services you use.

This privacy statement applies to websites and services of Microsoft that collect data and display these terms, as well as its offline product support services. It does not apply to those Microsoft sites, services and products that do not display or link to this statement or that have their own privacy statements. Some products, services or features mentioned in this statement may not be available in all markets at this time.

Collection of Your Personal Information
We collect information as part of operating our Websites and services.

- At some Microsoft sites, we ask you to provide personal information, such as your e-mail address, name, home or work address, or telephone number. We may also collect demographic information, such as your ZIP code, age, gender, preferences, interests and favorites. If you choose to make a purchase or sign up for a paid subscription service, we will ask for additional information, such as your credit card number and billing address.
- In order to access some Microsoft services, you will be asked to sign in with an e-mail address and password, which we refer to as your Windows Live ID. By signing in on one Microsoft site or service, you may be automatically signed into other Microsoft sites and services that use Windows Live ID. For more information, see the Windows Live ID privacy supplement.
- We collect additional information about your interaction with Microsoft sites and services without identifying you as an individual. For example, we receive certain standard information that your browser sends to every website you visit, such as your IP address, browser type and language, access times and referring Web site addresses. We also use Web site analytics tools on our sites to retrieve information from your browser, including the site you came from, the search engine(s) and the keywords you used to find our site, the pages you view within our site, your browser add-ons, and your browser's width and height.
- We use technologies, such as cookies and web beacons (described below), to collect information about the pages you view, the links you click and other actions you take on our sites and services.
- We also deliver advertisements (see the Display of Advertising section below) and provide Web site analytics tools on non-Microsoft sites and services, and we collect information about page views on these third party sites as well.
- When you receive newsletters or promotional e-mail from Microsoft, we may use web beacons (described below), customized links or similar technologies to determine whether the e-mail has been opened and which links you click in order to provide you more focused e-mail communications or other information.

Use of Your Personal Information
Microsoft collects and uses your personal information to operate and improve its sites and services. These uses include providing you with more effective customer service; making the sites or services easier to use by eliminating the need for you to repeatedly enter the same information; performing research and analysis aimed at improving our products, services and technologies; and displaying content and advertising that are customized to your interests and preferences. For more information about the use of information for advertising, see the Display of Advertising section below.

We also use your personal information to communicate with you. We may send certain mandatory service communications such as welcome letters, billing reminders, information on technical service issues, and security announcements. Some Microsoft services, such as Windows Live Hotmail, may send periodic member letters that are considered part of the service. Additionally, with your permission, we may also occasionally send you product surveys or promotional mailings to inform you of other products or services available from Microsoft and its affiliates, and/or share your personal information with Microsoft partners so they may send you information about their products and services. You can opt-out from receiving newsletters or promotional e-mail anytime by using this web form or by following the steps as described in the respective newsletter or promotional e-mail.

Personal information collected on Microsoft sites and services may be stored and processed in the United States or any other country in which Microsoft or its affiliates, subsidiaries or service providers maintain facilities. Microsoft abides by the safe harbor framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of data from the European Economic Area, and Switzerland.

Sharing of Your Personal Information
Except as described in this statement, we will not disclose your personal information outside of Microsoft and its controlled subsidiaries and affiliates without your consent. Some Microsoft sites allow you to choose to share your personal information with select Microsoft partners so that they can contact you about their products, services or offers. Other sites, such as MSN instead may give you a separate choice as to whether you wish to receive communications from Microsoft about a partner's particular offering (without transferring your personal information to the third party). See the Communication Preferences section below for more information.

Some Microsoft services are co-branded by Microsoft and another company (partner). If you register to or use such a service, both a Microsoft privacy statement and the partner’s privacy statement may be displayed. If so, both Microsoft and the partner will receive information you provide such as on registration forms.

Microsoft occasionally hires other companies (vendor) to provide limited services on our behalf, such as handling the processing and delivery of mailings, providing customer support, hosting websites, processing transactions, or performing statistical analysis of our services. Those service providers will be permitted to obtain only the personal information they need to deliver the service. They are required to maintain the confidentiality of the information and are prohibited from using it for any other purpose than for delivering the service to Microsoft in accordance with Microsoft’s instructions and policies. However, our vendors may use aggregate data for fraud detection to help improve their services. This helps them to more accurately detect fraudulent transactions. We may access or disclose information about you, including the

content of your communications, in order to: (a) comply with the law or respond to lawful requests or legal process; (b) protect the rights or property of Microsoft or our customers, including the enforcement of our agreements or policies governing your use of the services; or (c) act on a good faith belief that such access or disclosure is necessary to protect the personal safety of Microsoft employees, customers or the public. We may also disclose personal information as part of a corporate transaction such as a merger or sale of assets.

Display of Advertising (Opt-Out)
When we display online advertisements to you, we will place one or more persistent cookies on your computer or device in order to recognize your computer or device each time we display an ad to you. The information we collect includes, but may not be limited to, your computer's or device's IP address, our cookie IDs, browser type and language, operating system, website URLs, the specific ad posted on the site, and the date and time of delivery. If you click on the advertisement, we will also collect and store that action. Because we may serve advertisements on many different Web sites, we are able to compile information over time about where you, or others who are using your computer, saw and/or clicked on the advertisements we display. The cookies we use for delivering advertisements have an expiry date of no more than 2 years.

We may also place Web beacons (also called action tags or clear gifs) on our sites and in the advertisements we deliver, and we may provide our beacons to our advertising partners to place on their own Web sites. We may also include Web beacons in promotional e-mail messages or newsletters in order to determine whether messages have been opened and acted upon. Our beacons allow us to place or read our cookies and gather information about your subsequent visit, purchase or other activity on our sites and on the advertisers' Web sites. Microsoft and our advertising partners may use this information to determine the effectiveness of the advertisements and to show you ads based on your previous interactions with the site where the beacon is placed.

We use many different factors and types of information to select which advertisements to show you. For example, we may target some of the ads we display according to certain general interest categories or segments that we have inferred based on:

(a) the pages you view and links you click when using Microsoft's and its advertising partners' Web sites and services,
(b) the search terms you enter when using Microsoft's Internet search services, such as Bing,
(c) characteristics of the contacts you most frequently interact with through Microsoft's communications or social networking services, such as Messenger,
(d) demographic or interest data, including any you may have provided when creating a Windows Live ID (e.g. age, ZIP or postal code, gender),
(e) a general geographic location derived from your IP address, and/or
(f) demographic or interest data acquired from other companies (such as the population or other characteristics of the area where you live).

You may opt-out of receiving targeted ads from Microsoft Advertising by visiting our opt-out page. For more information about how Microsoft Advertising collects and uses information, please see the Microsoft Advertising Privacy Supplement.

We also allow third-party ad companies, including other ad networks, to display advertisements on our sites. In some cases, these third parties may also place cookies on your computer. These companies currently include, but are not limited to: 24/7 Real Media, aCerno,Inc, AdBlade, AdConion, AdFusion, Advertising.com, AppNexus, Bane Media, Brand.net,

CasaleMedia, Collective Media, Fox Interactive, Interclick, Millennial, PrecisionClick, ROI Media, Social Media, SpecificMedia, TrafficMarketplace, Tribal Fusion, ValueClick, Yahoo!, YuMe, and Zumobi. These companies may offer you a way to opt-out of ad targeting based on their cookies. You may find more information by clicking on the company names above and following the links to the Web sites of each company. Many of them are also members of the Network Advertising Initiative or the Digital Advertising Alliance, which each provide a simple way to opt-out of ad targeting from participating companies.

Security of Your Personal Information
Microsoft is committed to protecting the security of your personal information. We use a variety of security technologies and procedures to help protect your personal information from unauthorized access, use, or disclosure. For example, we store the personal information we collect on computer systems with limited access, which are located in controlled facilities. When we transmit highly confidential information (such as a credit card number or password) over the Internet, we protect it through the use of encryption, such as the Secure Socket Layer (SSL) protocol.

If a password is used to help protect your accounts and personal information, it is your responsibility to keep your password confidential. Do not share this information with anyone. If you are sharing a computer with anyone you should always log out before leaving a site or service to protect access to your information from subsequent users.

TRUSTe Certification
Microsoft has been awarded TRUSTe's Privacy Seal signifying that this privacy statement and our practices have been reviewed by TRUSTe for compliance with TRUSTe's program requirements including transparency, accountability and choice regarding the collection and use of your personal information. The TRUSTe program does not cover information that may be collected through downloadable software. TRUSTe's mission, as an independent third party, is to accelerate online trust among consumers and organizations globally through its leading privacy trustmark and innovative trust solutions.

ANNEX 12 MobileMe – Terms of Service

MOBILEME TERMS OF SERVICE

http://www.apple.com/legal/mobileme/en/terms.html

1. Your Acceptance of Terms

Updates
Apple may update or change these TOS from time to time and recommends that you review the TOS on a regular basis. You can review the most current version of the TOS at any time at http://www.apple.com/legal/mobileme/. If Apple makes a change to the TOS, it will post the revised TOS on our website at the link as herein noted. You understand and agree that your continued use of the Service after the TOS has changed constitutes your acceptance of the TOS as revised. Without limiting the foregoing, if Apple makes a change to the TOS that materially impacts your use of the Service, Apple may post notice of any such change on our website and/or email you notice of any such change to your MobileMe account.

2. Description of the Service

Changing the Service
Apple reserves the right to modify or stop the Service (or any part thereof), either temporarily or permanently, at any time or from time to time, with or without prior notice to you. Without limiting the foregoing, Apple may post on our website and/or send email to your MobileMe account, notice of such changes to the Service. It is your responsibility to review our website and/or check your MobileMe email address for any such notices. You agree that Apple shall not be liable to you or any third party for any modification or cessation of the Service.

Availability of the Service
The Service, or any feature or part thereof, may not be available in all languages or in all countries and Apple makes no representation that the Service, or any feature or part thereof, is appropriate or available for use in any particular location. To the extent you choose to access and use the Service, you do so at your own initiative and are responsible for compliance with any applicable laws, including, but not limited to, any applicable local laws.

3. Your Use of the Service

Sign Up Obligations
You agree that all information you provide to Apple during the sign up process ("Sign Up Data") will be true, accurate, complete and current information, and that you shall maintain and update the Sign Up Data as needed throughout your term to keep it accurate and current. Failure to provide accurate, current and complete Sign Up Data may result in the suspension and/or termination of your account.

4. Apple Privacy Policy

You understand that by using the Service, you consent and agree to the collection and use of certain information about you and your use of the Service in accordance with Apple's Privacy

Policy. You further consent and agree that Apple may collect, use, transmit, process and maintain information related to your account, and any devices registered thereunder, for purposes of providing the Service, and any features therein, to you. Information collected by Apple when you use the Service may also include technical or diagnostic information related to your use that may be used by Apple to maintain, improve and enhance the Service. For more information please read our full privacy policy at http://www.apple.com/legal/privacy/. You further understand and agree that this information may be transferred to the United States and/or other countries for storage, processing and use by Apple and/or its affiliates.

6. Payment

Automatic Renewal of Annual Subscription
When you sign up online for the Service, your annual subscription will be set to automatically renew upon its expiration. This means that unless you cancel your account or change its renewal settings prior to its expiration, your account will automatically renew for another year. At the time of renewal, we will charge your credit card the then-current fees to renew the Service. About thirty (30) days prior to your expiration date we will notify you by email to your MobileMe email address that your account is about to renew and remind you that your credit card will be billed the indicated Service fees on the renewal date. You may change your renewal settings at any time by going to https://secure.me.com/account.

Changes in Price
Apple may at any time, upon notice required by applicable law, change the price of the Service or any part thereof, or institute new charges or fees. Price changes and institution of new charges implemented during your subscription term will apply to subsequent subscription terms and to all new subscribers after the effective date of the change. If you do not agree to any such price changes, then you must cancel your account and stop using the Service. Your continued use of the Service after the effective date of any such change shall constitute your acceptance of such change.

7. Content Submitted or Made Available by You on the Service

License from You
Except for material we may license to you, Apple does not claim ownership of the materials and/or Content you submit or make available on the Service. However, by submitting or posting such Content on areas of the Service that are accessible by the public, you grant Apple a worldwide, royalty-free, non-exclusive license to use, distribute, reproduce, modify, adapt, publish, translate, publicly perform and publicly display such Content on the Service solely for the purpose for which such Content was submitted or made available. Said license will terminate within a commercially reasonable time after you or Apple remove such Content from the public area. By submitting or posting such Content on areas of the Service that are accessible by the public, you are representing that you are the owner of such material and/or have authorization to distribute it.

10. Termination

Termination by Apple
Apple may at any time, under certain circumstances and without prior notice, immediately terminate or suspend all or a portion of your account and/or access to the Service. Cause for such termination shall include, but not be limited to: (a) violations of the TOS or any other policies or guidelines that are referenced herein and/or posted on the Service; (b) a request by

you to cancel or terminate your account; (c) discontinuance or material modification to the Service or any part thereof; (d) a request and/or order from law enforcement, a judicial body, or other government agency; (e) where provision of the Service to you is or may become unlawful; (f) unexpected technical or security issues or problems; (g) your participation in fraudulent or illegal activities; or (h) failure to pay any fees owed by you in relation to the Service. Any such termination or suspension shall be made by Apple in its sole discretion, without any refund to you of any prepaid fees or amounts, and Apple will not be responsible to you or any third party for any damages that may result or arise out of such termination or suspension of your account and/or access to the Service.

12. Disclaimer of Warranties

SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, AS SUCH, TO THE EXTENT SUCH EXCLUSIONS ARE SPECIFICALLY PROHIBITED BY APPLICABLE LAW, SOME OF THE EXCLUSIONS SET FORTH BELOW MAY NOT APPLY TO YOU.

YOU EXPRESSLY UNDERSTAND AND AGREE THAT YOUR USE OF THE SERVICE IS AT YOUR SOLE RISK AND THE SERVICE IS PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS. APPLE AND ITS AFFILIATES, SUBSIDIARIES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, PARTNERS AND LICENSORS EXPRESSLY DISCLAIM ALL WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. IN PARTICULAR, APPLE AND ITS AFFILIATES, SUBSIDIARIES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, PARTNERS AND LICENSORS MAKE NO WARRANTY THAT (I) THE SERVICE WILL MEET YOUR REQUIREMENTS; (II) YOUR USE OF THE SERVICE WILL BE TIMELY, UNINTERRUPTED, SECURE OR ERROR-FREE; (III) ANY INFORMATION OBTAINED BY YOU AS A RESULT OF THE SERVICE WILL BE ACCURATE OR RELIABLE; AND (IV) ANY DEFECTS OR ERRORS IN THE SOFTWARE PROVIDED TO YOU AS PART OF THE SERVICE WILL BE CORRECTED.

ANY MATERIAL DOWNLOADED OR OTHERWISE OBTAINED THROUGH THE USE OF THE SERVICE IS ACCESSED AT YOUR OWN DISCRETION AND RISK, AND YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE TO YOUR DEVICE OR LOSS OF DATA THAT RESULTS FROM THE DOWNLOAD OF ANY SUCH MATERIAL. YOU FURTHER ACKNOWLEDGE THAT THE SERVICE IS NOT INTENDED OR SUITABLE FOR USE IN SITUATIONS OR ENVIRONMENTS WHERE THE FAILURE OR TIME DELAYS OF, OR ERRORS OR INACCURACIES IN, THE CONTENT, DATA OR INFORMATION PROVIDED BY THE SERVICE COULD LEAD TO DEATH, PERSONAL INJURY, OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE. NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED BY YOU FROM APPLE OR THROUGH OR FROM THE SERVICE SHALL CREATE ANY WARRANTY NOT EXPRESSLY STATED IN THE TOS.

13. Limitation of Liability

SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, AS SUCH, TO THE EXTENT SUCH EXCLUSIONS OR LIMITATIONS ARE SPECIFICALLY PROHIBITED BY APPLICABLE LAW, SOME OF THE EXCLUSIONS OR LIMITATIONS SET FORTH BELOW MAY NOT APPLY TO YOU. YOU EXPRESSLY UNDERSTAND AND AGREE THAT APPLE AND ITS AFFILIATES,

SUBSIDIARIES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, PARTNERS AND LICENSORS SHALL NOT BE LIABLE TO YOU FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES , INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, DATA, COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR OTHER INTANGIBLE LOSSES (EVEN IF APPLE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES), RESULTING FROM: (I) THE USE OR INABILITY TO USE THE SERVICE (II) ANY CHANGES MADE TO THE SERVICE OR ANY TEMPORARY OR PERMANENT CESSATION OF THE SERVICE OR ANY PART THEREOF; (III) THE UNAUTHORIZED ACCESS TO OR ALTERATION OF YOUR TRANSMISSIONS OR DATA; (IV) THE DELETION OF, CORRUPTION OF, OR FAILURE TO STORE AND/OR SEND OR RECEIVE YOUR TRANSMISSIONS OR DATA ON OR THROUGH THE SERVICE; (V) STATEMENTS OR CONDUCT OF ANY THIRD PARTY ON THE SERVICE; AND (VI) ANY OTHER MATTER RELATING TO THE SERVICE.

16. Governing Law

Except to the extent expressly provided in the following paragraph, these TOS and the relationship between you and Apple shall be governed by the laws of the State of California, excluding its conflicts of law provisions. You and Apple agree to submit to the personal and exclusive jurisdiction of the courts located within the county of Santa Clara, California, to resolve any dispute or claim arising from these TOS. If (a) you are not a U.S. citizen; (b) you do not reside in the U.S.; (c) you are not accessing the Service from the U.S.; and (d) you are a citizen of one of the countries identified below, you hereby agree that any dispute or claim arising from these TOS shall be governed by the applicable law set forth below, without regard to any conflict of law provisions, and you hereby irrevocably submit to the non-exclusive jurisdiction of the courts located in the state, province or country identified below whose law governs:

If you are a citizen of:	Governing law and forum:
Any European Union country	Laws of Republic of Ireland, Republic of Ireland

Specifically excluded from application to this Agreement is that law known as the United Nations Convention on the International Sale of Goods.

ANNEX 13 MobileMe – Privacy Policy

APPLE PRIVACY POLICY (MOBILEME)

http://www.apple.com/privacy/

Your privacy is important to Apple. So we've developed a Privacy Policy that covers how we collect, use, disclose, transfer, and store your information. Please take a moment to familiarize yourself with our privacy practices and let us know if you have any questions.

Collection and Use of Personal Information
Personal information is data that can be used to uniquely identify or contact a single person. You may be asked to provide your personal information anytime you are in contact with Apple or an Apple affiliated company. Apple and its affiliates may share this personal information with each other and use it consistent with this Privacy Policy. They may also combine it with other information to provide and improve our products, services, content, and advertising.
Here are some examples of the types of personal information Apple may collect and how we may use it.

What personal information we collect

- When you create an Apple ID, register your products, apply for commercial credit, purchase a product, download a software update, register for a class at an Apple Retail Store, or participate in an online survey, we may collect a variety of information, including your name, mailing address, phone number, email address, contact preferences, and credit card information.
- When you share your content with family and friends using Apple products, send gift certificates and products, or invite others to join you on Apple forums, Apple may collect the information you provide about those people such as name, mailing address, email address, and phone number.
- In the U.S., we may ask for your Social Security number (SSN) but only in limited circumstances such as when setting up a wireless account and activating your iPhone or when determining whether to extend commercial credit.

How we use your personal information

- The personal information we collect allows us to keep you posted on Apple's latest product announcements, software updates, and upcoming events. It also helps us to improve our services, content, and advertising. If you don't want to be on our mailing list, you can opt out anytime by updating your preferences.
- We also use personal information to help us develop, deliver, and improve our products, services, content, and advertising.
- From time to time, we may use your personal information to send important notices, such as communications about purchases and changes to our terms, conditions, and policies. Because this information is important to your interaction with Apple, you may not opt out of receiving these communications.
- We may also use personal information for internal purposes such as auditing, data analysis, and research to improve Apple's products, services, and customer communications.

- If you enter into a sweepstake, contest, or similar promotion we may use the information you provide to administer those programs.

Disclosure to Third Parties

At times Apple may make certain personal information available to strategic partners that work with Apple to provide products and services, or that help Apple market to customers. For example, when you purchase and activate your iPhone, you authorize Apple and its carrier to exchange the information you provide during the activation process to carry out service. If you are approved for service, your account will be governed by Apple and its carrier's respective privacy policies. Personal information will only be shared by Apple to provide or improve our products, services and advertising; it will not be shared with third parties for their marketing purposes.

Service Providers

Apple shares personal information with companies who provide services such as information processing, extending credit, fulfilling customer orders, delivering products to you, managing and enhancing customer data, providing customer service, assessing your interest in our products and services, and conducting customer research or satisfaction surveys. These companies are obligated to protect your information and may be located wherever Apple operates.

Protection of Personal Information

Apple takes precautions — including administrative, technical, and physical measures — to safeguard your personal information against loss, theft, and misuse, as well as against unauthorized access, disclosure, alteration, and destruction.

Apple online services such as the Apple Online Store and iTunes Store use Secure Sockets Layer (SSL) encryption on all web pages where personal information is collected. To make purchases from these services, you must use an SSL-enabled browser such as Safari, Firefox, or Internet Explorer. Doing so protects the confidentiality of your personal information while it's transmitted over the Internet.

When you use some Apple products, services, or applications or post on an Apple forum, chat room, or social networking service, the personal information you share is visible to other users and can be read, collected, or used by them. You are responsible for the personal information you choose to submit in these instances. For example, if you list your name and email address in a forum posting, that information is public. Please take care when using these features.

Our Companywide Commitment to Your Privacy

To make sure your personal information is secure, we communicate our privacy and security guidelines to Apple employees and strictly enforce privacy safeguards within the company.

Privacy Questions

If you have any questions or concerns about Apple's Privacy Policy or data processing, please contact us.

Apple may update its Privacy Policy from time to time. When we change the policy in a material way, a notice will be posted on our website along with the updated Privacy Policy.

Apple Inc., 1 Infinite Loop, Cupertino, California, USA 95014
Last updated: October 21, 2011

Apple Inc. has been awarded TRUSTe's Privacy Seal signifying that this Privacy Policy and practices have been reviewed by TRUSTe for compliance with TRUSTe's program requirements including transparency, accountability, and choice regarding the collection and use of your personal information. The TRUSTe program does not cover information that may be collected through downloadable software. If you have questions or complaints regarding our Privacy Policy or practices, please contact us. If you are not satisfied with our response, you can contact TRUSTe.

Privacy Questions

Questions or concerns about Apple's Privacy Policy or data processing?
Contact us

ANNEX 14 Yahoo! Security

SECURITY AT YAHOO!

http://info.yahoo.com/privacy/us/yahoo/security/

General
Yahoo! takes your security seriously and takes reasonable steps to protect your information. No data transmission over the Internet or information storage technology can be guaranteed to be 100% secure. The following is a summary of the measures Yahoo! takes to protect your information and descriptions of ways we implement these measures for different types of information you may provide to us. Please see the Yahoo! Security Center for additional information on how to reduce your security risk when online.

Yahoo! continues to evaluate and implement enhancements in security technology and practices, however we can only take steps to help reduce the risks of unauthorized access. Each individual using the Internet can take steps to help protect their information and further minimize the likelihood that a security incident may occur. We describe some of those measures and provide links to information that may be helpful in these pages and within the Yahoo! Security Center.

Security Steps We Have Taken

- Secure Socket Layer (SSL)
  Yahoo! uses SSL (Secure Socket Layer) encryption when transmitting certain kinds of information, such as financial services information or payment information. An icon resembling a padlock is displayed on the bottom of most browsers window during SSL transactions that involve credit cards and other forms of payment. Any time Yahoo! asks you for a credit card number on Yahoo! for payment or for verification purposes, it will be SSL encrypted. The information you provide will be stored securely on our servers. Once you choose to store or enter your credit card number on Yahoo!, it will not be displayed back to you in its entirety when you retrieve or edit it in the future. Instead of the entire number, you will only see asterisks and either the first four digits or the last four digits of your number.
- Security Key
  The Yahoo! Security Key is an additional optional layer of security to control access to sensitive information or services on Yahoo!. Users of financial services such as Yahoo! Wallet, Yahoo! Bill Pay, and Yahoo! Money Manager are asked to create a security key during the sign-up process or when you purchase certain services that require a Yahoo! Wallet. Please note that the Security Key automatically "times out" after an hour and requires the user to sign in again to access Security Key protected areas.
- Secure Storage
  Yahoo! maintains reasonable physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about you.
- Vendors and Partners
  Yahoo! works with vendors and partners to protect the security and privacy of user information.
- Employee and Contractor Access to Information

Yahoo! limits access to personal information about you to those employees who we reasonably believe need to come into contact with that information to provide products or services to you or in order to do their jobs.

- Education and Training for Employees
  Yahoo! has implemented a company-wide education and training program about security that is required of every Yahoo! employee.

Security Steps You Can Take

The following is information about topics that you may want to learn more about and steps you can take to help maintain your account and computer security when online.

- Ten Essential Security Tips
- About Passwords
- Choosing Your Password
- Password Scams
- Viruses, Trojan Horses and Worms
- Spyware
- Software
- Interacting Online With Strangers
- Shared Computer

ANNEX 15 Yahoo! — Terms of Service

YAHOO! CANADA TERMS OF SERVICE

http://info.yahoo.com/legal/ca/yahoo/utos/utos-ca01.html

DESCRIPTION OF SERVICE
Yahoo! currently provides users with access to a rich collection of resources, including, various communications tools, forums, shopping services, search services, personalized content and branded programming through its network of properties which may be accessed through various mediums or devices now known or hereafter developed (the "**Service**"). You understand and agree that the Service may include advertisements and that these advertisements are necessary for Yahoo! to provide the Service. You understand and agree that the Service may include certain communications from Yahoo!, such as service announcements and administrative messages that are considered part of the Yahoo! Membership, and that you cannot opt out of receiving them. Unless explicitly stated otherwise, any new features that augment or enhance the current Service, including the release of new Yahoo! properties, are subject to the TOS. You understand and agree that the Service is provided "AS-IS" and that Yahoo! assumes no responsibility for the timeliness, deletion, mis-delivery or failure to store any user communications or personalization settings.

You are responsible for obtaining access to the Service and that access may involve third party fees (such as Internet service provider or airtime charges). You are responsible for those fees, including fees associated with the display or delivery of advertisements. In addition, you must provide and are responsible for all equipment necessary to access the Service.

Please be aware that Yahoo! has created certain areas on the Service that contain adult or mature content. You must have attained the age of majority in the province or territory in which you live to access such areas on the Service.

YOUR REGISTRATION OBLIGATIONS
In consideration of your use of the Service, you represent that you are of legal age to form a binding contract and are not a person barred from receiving services under the laws of Canada or other applicable jurisdictions. You also agree to: (a) provide true, accurate, current and complete information about yourself as prompted by the Service's registration form (such information being the "**Registration Data**") and (b) maintain and promptly update the Registration Data to keep it true, accurate, current and complete. If you provide any information that is untrue, inaccurate, not current or incomplete, or Yahoo! has reasonable grounds to suspect that such information is untrue, inaccurate, not current or incomplete, Yahoo! has the right to suspend or terminate your account and refuse any and all current or future use of the Service (or any portion thereof).

Yahoo! is concerned about the safety and privacy of all its users, particularly children. For this reason, parents who wish to allow their children access to the Service should assist them in setting up any relevant accounts and supervise their access to the Service. By allowing your child access to the Service, they will be able to access all of the Services including, email, message boards, groups, instant messages and chat (among others). Please remember that the Service is designed to appeal to a broad audience. Accordingly, as the legal guardian, it is

your responsibility to determine whether any of the Services and/or Content (as defined in Section 6 below) are appropriate for your child.

YAHOO PRIVACY POLICY
Registration Data and certain other information about you is subject to our Privacy Policy. For more information, see our full privacy policy at http://privacy.yahoo.com/privacy/ca/. You understand that through your use of the Service you consent to the collection, use and disclosure of this information, only as permitted by the Privacy Policy, including the transfer of this information to the United States and/or other countries for storage, processing, and use by Yahoo! and its affiliates in order to provide the Service to you.

The Yahoo! I.D. associated with your account is the property of Yahoo! or its affiliates, and is not your personal information.

CONTENT SUBMITTED OR MADE AVAILABLE FOR INCLUSION ON THE SERVICE
Yahoo! does not claim ownership of Content you submit or make available for inclusion on the Service. However, with respect to Content you submit or make available for inclusion on publicly accessible areas of the Service, you grant Yahoo! the following world-wide, royalty free and non-exclusive license(s), as applicable:

- With respect to Content you submit or make available for inclusion on publicly accessible areas of Yahoo! Groups, the license to use, distribute, reproduce, modify, adapt, publicly perform, and publicly display such Content on the Service solely for the purposes of providing and promoting the specific Yahoo! Group to which such Content was submitted or made available. This licence exists only for as long as you elect to continue to include such Content on the Service and will terminate at the time you remove or Yahoo! removes such Content from the Service.
- With respect to photos, graphics, audio, or video you submit or make available for inclusion on publicly accessible areas of the Service other than Yahoo! Groups, the license to use, distribute, reproduce, modify, adapt, publicly perform and publicly display such Content on the Service solely for the purpose for which such Content was submitted or made available. This licence exists only for as long as you elect to continue to include such Content on the Service and will terminate at the time you remove or Yahoo! removes such Content from the Service.
- With respect to Content other than photos, graphics, audio or video you submit or make available for inclusion on publicly accessible areas of the Service other than Yahoo! Groups, the perpetual, irrevocable and fully sublicensable license to use, distribute, reproduce, modify, adapt, publish, translate, publicly perform and publicly display such Content (in whole or in part) and to incorporate such Content into other works in any format or medium now known or later developed.

You irrevocably waive any moral rights or other rights with respect to attribution of authorship or integrity in the Content you submit.

Publicly accessible" areas of the Service are those areas of the Yahoo! network of properties that are intended by Yahoo! to be available to the general public. By way of example, publicly accessible areas of the Service would include Yahoo! Message Boards and portions of Yahoo! Groups, Photos and Briefcase that are open to both members and visitors. However, publicly accessible areas of the Service would not include portions of Yahoo! Groups, Photos, and Briefcase that are limited to members or visitors, Yahoo! services intended for private communication such as Yahoo! Mail or Yahoo! Messenger, or areas off of the Yahoo! network

of properties such as portions of World Wide Web sites that are accessible through hypertext or other links but are not hosted or served by Yahoo!.

INDEMNITY
You agree to indemnify and hold Yahoo! and its subsidiaries, affiliates, officers, employees, agents, co-branders, partners and licensors harmless from any claim or demand, including reasonable legal fees, made by any third party due to or arising out of Content you submit, post, transmit or make available through the Service, your use of the Service, your connection to the Service, your violation of the TOS, or your violation of any rights of another.

MODIFICATIONS TO SERVICE
Yahoo! reserves the right at any time to modify or discontinue, temporarily or permanently, the Service (or any part thereof) with or without notice. You agree that Yahoo! will not be liable to you or to any third party for any modification, suspension or discontinuance of the Service.

TERMINATION AND RECYCLING OF ACCOUNTS
You agree that Yahoo!, in its sole discretion, may terminate your account or any part thereof, including any associated email address or your use of the Service, and remove and discard any Content within the Service, for any reason, including, without limitation, (a) lack of use, (b) if Yahoo! believes that you have violated or acted inconsistently with the letter or spirit of the TOS or other incorporated agreements or guidelines, (c) requests by law enforcement or other government agencies, (d) a request by you (self-initiated account deletions), (e) discontinuance or material modification to the Service (or any part thereof), (f) unexpected technical or security issues or problems, (g) in compliance with legal process; (h) if you have or we believe you have engaged in illegal activities, including without limitation, fraud, and/or (i) nonpayment of any fees owed by you in connection with the Services. Yahoo! may also, in its sole discretion and at any time, discontinue providing the Service, or any part thereof, with or without notice. You acknowledge and agree that any termination of your access to the Service under any provision of this TOS may be effected without prior notice and that Yahoo! may immediately deactivate or delete your account and all related Content (including without limitation email messages and photos)) associated with or stored in your account and/or bar any further access to such Content or the Service. Further, you agree that Yahoo! is not liable to you or any third-party for termination of your account (including any associated email address), or termination of your access to the Service.

As Yahoo! IDs and the related email addresses are the property of Yahoo!, upon termination of your account the Yahoo! I.D. or email address previously associated with your account will become available to other Yahoo! users to select as their Yahoo! I.D. While Yahoo! will take reasonable steps as described in our Privacy Policy to secure the information provided by you prior to the termination of your account, you understand and agree that it is solely your responsibility and obligation to notify others that you no longer can be contacted at a particular terminated Yahoo! I.D. or email address. You expressly acknowledge and agree that you, and not Yahoo!, are solely responsible for the receipt of correspondence erroneously directed to you at your terminated Yahoo! I.D. or email address that may now belong to another Yahoo! user.

DISCLAIMER OF WARRANTIES, REPRESENTATIONS, AND CONDITIONS

YOU EXPRESSLY UNDERSTAND AND AGREE THAT:

d. YOUR USE OF THE SERVICE IS AT YOUR SOLE RISK. THE SERVICE IS PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS. YAHOO! AND ITS SUBSIDIARIES, AFFILIATES, OFFICERS, EMPLOYEES, AGENTS, CO-BRANDERS,

PARTNERS AND LICENSORS EXPRESSLY DISCLAIMS ALL WARRANTIES, REPRESENTATIONS AND CONDITIONS OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES, REPRESENTATIONS AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.

e. YAHOO! AND ITS SUBSIDIARIES, AFFILIATES, OFFICERS, EMPLOYEES, AGENTS, CO-BRANDERS, PARTNERS AND LICENSORS MAKES NO WARRANTY THAT (i) THE SERVICE WILL MEET YOUR REQUIREMENTS, (ii) THE SERVICE WILL BE UNINTERRUPTED, TIMELY, SECURE, OR ERROR-FREE, (iii) THE RESULTS THAT MAY BE OBTAINED FROM THE USE OF THE SERVICE WILL BE ACCURATE OR RELIABLE, (iv) THE QUALITY OF ANY PRODUCTS, SERVICES, INFORMATION, OR OTHER MATERIAL PURCHASED OR OBTAINED BY YOU THROUGH THE SERVICE WILL MEET YOUR EXPECTATIONS, AND (V) ANY ERRORS IN THE SOFTWARE WILL BE CORRECTED.
f. ANY MATERIAL DOWNLOADED OR OTHERWISE OBTAINED THROUGH THE USE OF THE SERVICE IS DONE AT YOUR OWN DISCRETION AND RISK AND THAT YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE TO YOUR COMPUTER SYSTEM OR LOSS OF DATA THAT RESULTS FROM THE DOWNLOAD OF ANY SUCH MATERIAL.
g. NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED BY YOU FROM YAHOO! OR THROUGH OR FROM THE SERVICE SHALL CREATE ANY WARRANTY NOT EXPRESSLY STATED IN THE TOS.

LIMITATION OF LIABILITY
YOU EXPRESSLY UNDERSTAND AND AGREE THAT YAHOO! AND ITS SUBSIDIARIES, AFFILIATES, OFFICERS, EMPLOYEES, AGENTS, CO-BRANDERS, PARTNERS AND LICENSORS SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES, INCLUDING BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, DATA, OR OTHER INTANGIBLE LOSSES (EVEN IF YAHOO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES), RESULTING FROM: (i) THE USE OR THE INABILITY TO USE THE SERVICE; (ii) THE COST OF PROCUREMENT OF SUBSTITUTE GOODS AND SERVICES RESULTING FROM ANY GOODS, DATA, INFORMATION, OR SERVICES PURCHASED OR OBTAINED OR MESSAGES RECEIVED OR TRANSACTIONS ENTERED INTO THROUGH OR FROM THE SERVICE; (iii) UNAUTHORIZED ACCESS TO OR ALTERATION OF YOUR TRANSMISSIONS OR DATA; (iv) STATEMENTS OR CONDUCT OF ANY THIRD PARTY ON THE SERVICE; OR (v) ANY OTHER MATTER RELATING TO THE SERVICE.

EXCLUSIONS AND LIMITATIONS
SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, REPRESENTATIONS AND CONDITIONS OR THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES. ACCORDINGLY, SOME OF THE ABOVE LIMITATIONS OF SECTIONS 18 AND 19 MAY NOT APPLY TO YOU.

NOTICE
Notices to you may be made via either email or regular mail. The Service may also provide notices of changes to the TOS or other matters by displaying notices or links to notices to you on the Service.

From time to time Yahoo! will send you notices through the Yahoo! Messenger Service to let you know about important changes to the Yahoo! Messenger or related Services. Such

messages may not be received if you violate this TOS by accessing the Service in an unauthorized manner. Your agreement to this TOS constitutes your agreement that you are deemed to have received any and all notices that would have been delivered had you accessed the Service in an authorized manner.

GENERAL INFORMATION

Choice of Law and Forum. The TOS and the relationship between you and Yahoo! shall be governed by the laws of the province of Ontario and Canada without regard to its conflict of law provisions. You and Yahoo! agree to submit to the personal and exclusive jurisdiction of the courts located within the province of Ontario, Canada.

Waiver and Severability of Terms. The failure of Yahoo! to exercise or enforce any right
Language. The parties hereto have agreed that this Agreement and any of its accessories, including notice, be written in the English language.

ANNEX 16 Yahoo! – Privacy Policy

YAHOO! PRIVACY POLICY

http://info.yahoo.com/privacy/ca/yahoo/

WHAT THIS PRIVACY POLICY COVERS

Yahoo! takes your privacy seriously. Please read the following to learn more about our privacy policy.

This policy covers how Yahoo! treats personal information that Yahoo! collects and receives, including information related to your past use of Yahoo! products and services. Personal information is information about an identifiable individual like your name, email address or phone number and that is not otherwise publicly available.

This privacy policy only applies to Yahoo! This policy does not apply to the practices of companies that Yahoo! does not own or control, or to people that Yahoo! does not employ or manage. In addition, some companies that Yahoo! has acquired have their own, preexisting privacy policies which may be viewed on the Yahoo! acquired companies page.

INFORMATION COLLECTION AND USE

General

Yahoo! collects personal information when you register with Yahoo!, when you use Yahoo! products or services, when you visit Yahoo! pages or the pages of certain Yahoo! partners, and when you enter promotions or sweepstakes. Yahoo! may combine information about you that we have with information we obtain from business partners or other companies.

When you register we ask for information such as your name, gender, birth date, postal code and email address. Once you register with Yahoo! and sign in to our services, you are not anonymous to us.

Yahoo! collects information about your transactions with us and with some of our business partners, including information about your use of financial products and services that we offer.

Yahoo! automatically receives and records information from your computer and browser, including your IP address, Yahoo! cookie information, software and hardware attributes, and the page you request.

Yahoo! uses information for the following general purposes: to customize the advertising and content you see, fulfill your requests for products and services, improve our services, contact you, conduct research, and provide anonymous reporting for internal and external clients.

INFORMATION SHARING AND DISCLOSURE

Yahoo! does not rent, sell, or share personal information about you with other people or non-affiliated companies except to provide products or services you've requested, when we have your permission, or under the following circumstances:

- We provide the information to trusted partners who work on behalf of or with Yahoo! under confidentiality agreements. These companies may use your personal information to help

Yahoo! communicate with you about offers from Yahoo! and our marketing partners. However, these companies do not have any independent right to share this information.
- When you register for a Yahoo! account, your registration information and other data will be transmitted to the United States and/or other countries for processing and storage by Yahoo! and its affiliates. In addition, we may provide your personal information to a Yahoo! affiliate worldwide for the general purposes described above under “Information Collection and Use.” For example, various Yahoo! affiliates may be responsible for processing and storing your information in order to deliver content and services to you. In these situations your information may be subject to the legal jurisdiction of these countries.
- We respond to disclosure demands if permitted or required by law including responding to warrants, subpoenas, court orders, or other legal process, or to establish or exercise our legal rights or defend against legal claims.
- We believe it is necessary to share information in order to investigate, prevent, or take action regarding illegal activities including suspected fraud, situations involving potential threats to the physical safety of any person, violations of Yahoo!'s terms of use, or as otherwise required by law. We transfer information about you if Yahoo! is acquired by or merged with another company. In this event, Yahoo! will notify you before information about you is transferred and becomes subject to a different privacy policy.

Yahoo! displays targeted advertisements based on personal information. Advertisers (including ad serving companies) may assume that people who interact with, view, or click targeted ads meet the targeting criteria—for example, women ages 18-24 from a particular geographic area.
- Yahoo! does not provide any personal information to the advertiser when you interact with or view a targeted ad. However, by interacting with or viewing an ad you are consenting to the possibility that the advertiser will make the assumption that you meet the targeting criteria used to display the ad.
- Yahoo! advertisers include financial service providers (such as banks, insurance agents, stock brokers and mortgage lenders) and non-financial companies (such as stores, airlines, and software companies).

Yahoo! works with vendors, partners, advertisers, and other service providers in different industries and categories of business. For more information regarding providers of products or services that you've requested please read our detailed reference links.

CONFIDENTIALITY AND SECURITY

We limit access to personal information about you to employees who we believe reasonably need to come into contact with that information to provide products or services to you or in order to do their jobs.

We have physical, electronic, and procedural safeguards that comply with our legal obligations to protect personal information about you.

To learn more about security, including the security steps we have taken and security steps you can take, please read Security at Yahoo!.

ANNEX 17 Zoho – Privacy Policy

ZOHO PRIVACY POLICY

Last Updated: 16th April 2010

http://www.zoho.com/privacy.html

General
ZOHO Corporation is a Licensee of the TRUSTe Privacy Program. TRUSTe is an independent organization whose mission is to build users' trust and confidence in the internet by promoting the use of fair information practices. As a testament of our commitment to your privacy, we have elected to disclose our information practices and have our privacy practices reviewed for compliance by TRUSTe. Please direct all your inquiries pertaining to this Privacy Policy Statement or the service to us at the contact information below.

Information Recorded and Use:

- **Personal Information**
  During the Registration Process for creating a user account, we request for your name and email address. You will also be asked to choose a unique username and a password, which will be used solely for the purpose of providing access to your user account. Upon registration you will have the option of choosing a security question and an answer to the security question, which if given, will be used solely for the purpose of resetting your password. Your name and email address will be used to inform you regarding new services, releases, upcoming events and changes in this Privacy Policy Statement. When you elect to sign up for a user account, you also have the option to create the user account using any of the trusted third party user authentication services integrated with Zoho Services . In doing so, no Personal Information within your third party email accounts is transferred to your user account without your explicit consent.

  Zoho will have access to third party personal information provided by you as part of using Zoho Services such as contacts in your Zoho Mail account. This information may include third party names, email addresses, phone numbers and physical addresses and will be used for servicing your requirements as expressed by you to Zoho and solely as part and parcel of your use of Zoho Services. We do not share this third party personal information with anyone for promotional purposes, nor do we utilize it for any purposes not expressly consented to by you. When you elect to refer friends to the website, we request their email address and name to facilitate the request and deliver this one time email.

  We post user testimonials on the website. These testimonials may include names and we acquire permission from our users prior to posting these on the website. Zoho is not responsible for the Personal Information users elect to post within their testimonials.

- **Usage Details**
  Your usage details such as time, frequency, duration and pattern of use, features used and the amount of storage used will be recorded by us in order to enhance your experience of the Zoho services and to help us provide you the best possible service.

- **Contents of your User Account**
  We store and maintain files, documents, to-do lists, emails and other data stored in your user account at our facilities in the United States or any other country. Use of Zoho Services signifies your consent to such transfer of your data outside of your country. In order to prevent loss of data due to errors or system failures, we also keep backup copies of data including the contents of your user account. Hence your files and data may remain on our servers even after deletion or termination of your user account. We assure you that the contents of your user account will not be disclosed to anyone and will not be accessible even to employees of Zoho except in circumstances specifically mentioned in this Privacy Policy Statement. We also do not process the contents of your user account for serving targeted advertisements.

With whom we share Information
We may need to disclose Personal Information to our affiliates, service providers and business partners solely for the purpose of providing Zoho Services to you. In such cases Zoho will also ensure that such affiliates, service providers and business partners comply with this Privacy Policy Statement and adopt appropriate confidentiality and security measures. We will obtain your prior specific consent before we share or disclose your Personal Information to any person outside Zoho for any purpose that is not directly connected with providing Zoho Services to you. We may share generic aggregated demographic information not linked to any Personal Information regarding visitors and users with our business partners and advertisers. Please be aware that laws in various jurisdictions in which we operate may obligate us to disclose user information and the contents of your user account to the local law enforcement authorities under a legal process or an enforceable government request. In addition, we may also disclose Personal Information and contents of your user account to law enforcement authorities if such disclosure is determined to be necessary by Zoho in our sole and absolute discretion for protecting the safety of our users, employees, or the general public.

How secure is your Information
We adopt industry appropriate data collection, storage and processing practices and security measures, as well as physical security measures to protect against unauthorized access, alteration, disclosure or destruction of your Personal Information, username, password, transaction information and data stored in your user account. Access to your name and email address is restricted to our employees who need to know such information in connection with providing Zoho Services to you and are bound by confidentiality obligations.

Your Choice in Information Use
You will be required to register for our Zoho Services by providing Personal Information. If you choose not to provide your Personal Information, we will be unable to provide you the Zoho Services. We do provide you with the option of not choosing a secret question and the answer to it; however, we may not be able to reset your password for you. We also provide you with the option of opting out from receiving mail from us; however, you will not be able to receive email notifications of new services, releases, upcoming events and changes to the Privacy Policy Statement should you decide to opt-out of receiving all messages from Zoho. In the event we decide to use your Personal Information for any purpose other than as stated in this Privacy Policy Statement, we will offer you an effective way to opt out of the use of your Personal Information for those other purposes. You may opt out of receiving newsletters and other secondary messages from Zoho by selecting the ‘unsubscribe’ function present in every message we send.

ANNEX 18 Zoho – Terms of Service

ZOHO TERMS OF SERVICES

THIS IS AN AGREEMENT BETWEEN YOU OR THE ENTITY THAT YOU REPRESENT (hereinafter "You" or "Your") AND ZOHO CORPORATION (hereinafter "Zoho") GOVERNING YOUR USE OF ZOHO SUITE OF ONLINE BUSINESS PRODUCTIVITY AND COLLABORATION SOFTWARE (hereinafter "Zoho Service(s)").

http://www.zoho.com/terms.html

Modification of Terms of Service
We may modify the Terms upon notice to you at any time. You will be provided notice of any such modification by electronic mail or by publishing the changes on the website http://zoho.com/terms.html. You may terminate your use of the Services if the Terms are modified in a manner that substantially affects your rights in connection with use of the Services. Your continued use of the Service after notice of any change to the Terms will be deemed to be your agreement to the amended Terms.

Personal Information and Privacy
Personal information you provide to Zoho through the Service is governed by Zoho Privacy Policy. Your election to use the Service indicates your acceptance of the terms of the Zoho Privacy Policy. You are responsible for maintaining confidentiality of your username, password and other sensitive information. You are responsible for all activities that occur in your user account and you agree to inform us immediately of any unauthorized use of your user account by email to accounts@zohocorp.com or by calling us on any of the numbers listed on http://www.zoho.com/contact.html. We are not responsible for any loss or damage to you or to any third party incurred as a result of any unauthorized access and/or use of your user account, or otherwise.

Data Ownership
We respect your right to ownership of content created or stored by you. You own the content created or stored by you. Unless specifically permitted by you, your use of the Services does not grant Zoho the license to use, reproduce, adapt, modify, publish or distribute the content created by you or stored in your user account for Zoho's commercial, marketing or any similar purpose. But you grant Zoho permission to access, copy, distribute, store, transmit, reformat, publicly display and publicly perform the content of your user account solely as required for the purpose of providing the Services to you.

User Generated Content
You may transmit or publish content created by you using any of the Services or otherwise. However, you shall be solely responsible for such content and the consequences of its transmission or publication. Any content made public will be publicly accessible through the internet and may be crawled and indexed by search engines. You are responsible for ensuring that you do not accidentally make any private content publicly available. Any content that you may receive from other users of the Services, is provided to you AS IS for your information and personal use only and you agree not to use, copy, reproduce, distribute, transmit, broadcast, display, sell, license or otherwise exploit such content for any purpose, without the express

written consent of the person who owns the rights to such content. In the course of using any of the Services, if you come across any content with copyright notice(s) or any copy protection feature(s), you agree not to remove such copyright notice(s) or disable such copy protection feature(s) as the case may be. By making any copyrighted/copyrightable content available on any of the Services you affirm that you have the consent, authorization or permission, as the case may be from every person who may claim any rights in such content to make such content available in such manner. Further, by making any content available in the manner aforementioned, you expressly agree that Zoho will have the right to block access to or remove such content made available by you, if Zoho receives complaints concerning any illegality or infringement of third party rights in such content. By using any of the Services and transmitting or publishing any content using such Service, you expressly consent to determination of questions of illegality or infringement of third party rights in such content by the agent designated by Zoho for this purpose.

For procedure relating to complaints of illegality or infringement of third party rights in content transmitted or published using the Services, click here.

If you wish to protest any blocking or removal of content by Zoho, you may do so in the manner provided here.

Disclaimer of Warranties
YOU EXPRESSLY UNDERSTAND AND AGREE THAT THE USE OF THE SERVICES IS AT YOUR SOLE RISK. THE SERVICES ARE PROVIDED ON AN AS-IS-AND-AS-AVAILABLE BASIS. ZOHO EXPRESSLY DISCLAIMS ALL WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ZOHO MAKES NO WARRANTY THAT THE SERVICES WILL BE UNINTERRUPTED, TIMELY, SECURE, OR VIRUS FREE. USE OF ANY MATERIAL DOWNLOADED OR OBTAINED THROUGH THE USE OF THE SERVICES SHALL BE AT YOUR OWN DISCRETION AND RISK AND YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE TO YOUR COMPUTER SYSTEM, MOBILE TELEPHONE, WIRELESS DEVICE OR DATA THAT RESULTS FROM THE USE OF THE SERVICES OR THE DOWNLOAD OF ANY SUCH MATERIAL. NO ADVICE OR INFORMATION, WHETHER WRITTEN OR ORAL, OBTAINED BY YOU FROM ZOHO, ITS EMPLOYEES OR REPRESENTATIVES SHALL CREATE ANY WARRANTY NOT EXPRESSLY STATED IN THE TERMS.

Limitation of Liability
YOU AGREE THAT ZOHO SHALL, IN NO EVENT, BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR OTHER LOSS OR DAMAGE WHATSOEVER OR FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, COMPUTER FAILURE, LOSS OF BUSINESS INFORMATION, OR OTHER LOSS ARISING OUT OF OR CAUSED BY YOUR USE OF OR INABILITY TO USE THE SERVICE, EVEN IF ZOHO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. YOUR SOLE AND EXCLUSIVE REMEDY FOR ANY DISPUTE WITH ZOHO RELATED TO ANY OF THE SERVICES SHALL BE TERMINATION OF SUCH SERVICE. IN NO EVENT SHALL ZOHO'S ENTIRE LIABILITY TO YOU IN RESPECT OF ANY SERVICE, WHETHER DIRECT OR INDIRECT, EXCEED THE FEES PAID BY YOU TOWARDS SUCH SERVICE.

Indemnification
You agree to indemnify and hold harmless Zoho, its officers, directors, employees, suppliers, and affiliates, from and against any losses, damages, fines and expenses (including attorney's fees and costs) arising out of or relating to any claims that you have used the Services in violation of another party's rights, in violation of any law, in violations of any provisions of the Terms, or any other claim related to your use of the Services, except where such use is authorized by Zoho.

Arbitration
Any controversy or claim arising out of or relating to the Terms shall be settled by binding arbitration in accordance with the commercial arbitration rules of the American Arbitration Association. Any such controversy or claim shall be arbitrated on an individual basis, and shall not be consolidated in any arbitration with any claim or controversy of any other party. The decision of the arbitrator shall be final and unappealable. The arbitration shall be conducted in California and judgment on the arbitration award may be entered into any court having jurisdiction thereof. Notwithstanding anything to the contrary, Zoho may at any time seek injunctions or other forms of equitable relief from any court of competent jurisdiction.

Suspension and Termination
We may suspend your user account or temporarily disable access to whole or part of any Service in the event of any suspected illegal activity, extended periods of inactivity or requests by law enforcement or other government agencies. Objections to suspension or disabling of user accounts should be made to legal@zohocorp.com within thirty days of being notified about the suspension. We may terminate a suspended or disabled user account after thirty days. We will also terminate your user account on your request. In addition, we reserve the right to terminate your user account and deny the Services upon reasonable belief that you have violated the Terms and to terminate your access to any Beta Service in case of unexpected technical issues or discontinuation of the Beta Service. Termination of user account will include denial of access to all Services, deletion of information in your user account such as your e-mail address and password and deletion of all data in your user account.

ANNEX 19 ZumoDrive – Privacy Policy

ZUMO DRIVE PRIVACY POLICY

http://www.zumodrive.com/privacy

Information We Collect from You
When you use the Services, we collect personal information from you and about you. Personal information refers to information that can be used to contact or identify you and information on your use of the Services. Personal information that we collect include, but is not limited to, your name, email addresses, credit card or other payment method information, telephone numbers, home, business, and/or billing postal addresses, email contacts (names and email addresses), IP addresses, preferences and settings, and activities and the date and time of activities performed during the use of the Services.

Our servers also automatically collect information about your computer and your visits to the website, such as your IP address, browser type, date and time of visit, length of visit, page views, and the date and time of each page view in the server log files.

Similar to many other websites, the website utilizes a standard technology called "cookies" to collect and store information for record-keeping purposes in a part of your computer hard drive specifically designed for cookies. A cookie is a very small data file, which often includes an anonymous unique identifier. When you visit the website, the web server asks your browser for permission to store this file on your computer. If your browser does not accept cookies, you may not be able to use all functionality of the website. We use cookies to save your sign-in ID and password for future sign-ins to the website; and we use cookies to enable certain features of the website, to better understand how you interact with the website and to monitor aggregate usage and web traffic routing on the website.

In addition to personal information, we also collect “aggregate” information, which we collect from all our users as a group over time and which does not contain user identity information. We may use third parties to collect such aggregate information, and we may share aggregate information with third information with third parties for various purposes, including helping us better understand our users and improve the Services.

How We Use Personal Information
We use your personal information for the following purposes: (a) to provide and improve the Services for you, (b) to administer your account and use of the Services, (c) to determine files and folders owned or added by you and shared with you, (d) to track and report your file and folder activities, (e) to personalize your experience during your use of the Services, (f) to authenticate your use of the Services, (g) to allow others to share files and folders with you, (h) to allow others to communicate with you using the Services, (i) to allow us to provide you software and product updates, and (j) to aggregate user metric or summary information for us to monitor and analyze the use of the Services.

How We Use Aggregate Information
We use information we aggregate by various means as described above for the following purposes: (a) to monitor and analyze the use of the Services, (b) to administer and monitor the capacity of our servers, (c) to ensure acceptable performance of our servers, (d) to help us identify and prioritize new features to develop and add to the Services, and (e) to help us understand the scope of any service issue

How We Share and Disclose Information
When you share a file or folder with or send a message about a file or folder to other users, they will see a limited portion of your personal information just enough for them to recognize who you are. This limited portion includes, but is not limited to, your name and email address. When you perform activities to a file or folder you have shared with others or have been shared with you by others, the summary of such activities are displayed to other users and they include your name.

We also use third parties (service providers, consultants, partners, etc.) to facilitate the Services, including, but not limited to, sending email, processing payments, providing computing servers, storing data and personal information, managing databases, and monitoring and analyzing the performance, reliability, and user experience of the Services. In connection with these business operations, these third parties may have access to your personal information for use in connection with their business activities and tasks on our behalf. As we develop our business, we may buy or sell assets or business offerings. Personal and aggregate information is generally one of the transferred business assets in these types of transactions. We may also transfer such information in the course of corporate divestitures, mergers, or any dissolution.

Security
At Zecter, Inc. we strive to implement reasonable measures to prevent unauthorized access, modification, destruction, or damage of your personal information and data stored using the Services. At your choice, your data stored in our servers is encrypted using Advanced Encryption Standard and, when transmitted over the network, is protected with SSL encryption. Our servers are running in a secure environment. Your information and data and our application and server data are backed up. While we have taken efforts to protect and secure your information and data, we cannot guarantee that your information and data will not be disclosed or accessed by accidental circumstances or by the unauthorized acts of others.

Your account, information, data, and access to the Services is authenticated only by the use of your correct sign-in ID and password. You must keep your password confidential and not share it to any other person. You are responsible for the use of the Services by any other person using your sign-in ID and password.

ANNEX 20 ZumoDrive – Terms of Service

ZUMODRIVE TERMS OF SERVICE

By using the ZumoDrive.com web site and any ZumoDrive desktop and mobile software ("**Service**") of Zecter, Inc. ("**Company**"), you are agreeing to be bound by the following terms and conditions ("**Terms of Service**"). Violation of any of the terms below will result in the termination of your Account.

Company reserves the right to update and change the Terms of Service from time to time without notice. Any new features that augment or enhance the current Service, including the release of new tools and resources, will be subject to the Terms of Service. Continued use of the Service after any such changes will constitute your consent to such changes. You can review the most current version of the Terms of Service at any time at: http://www.zumodrive.com/tos

Copyright and Content Ownership

1. You will share User Files: (i) that you have the lawful right to use, copy, distribute, transmit, or display; and (ii) that do not infringe the intellectual property rights or violate the privacy rights of any third party (including, without limitation, copyright, trademark, patent, trade secret, or other intellectual property right).
2. We claim no intellectual property rights over User Files. Your profile and any User Files stored and/or shared remain yours. However, by sharing User Files through the Service, you agree to allow others to view, edit, and/or share your User Files.
3. Company has the right (but not the obligation) in its sole discretion to refuse or remove any User Files that are shared via the Service.

General Conditions

1. You use the Service is at your own risk. The service is provided on an "as is" and "as available" basis.
2. You understand that Company uses third party vendors and hosting partners to provide the necessary hardware, software, networking, storage, and related technology required to run the Service.
3. You must not modify, adapt or hack the Service or modify another website so as to falsely imply that it is associated with the Service or Company.
4. You agree not to reproduce, duplicate, copy, sell, resell or exploit any portion of the Service, use of the Service, or access to the Service without the prior written permission of Company.
5. You understand that the technical processing and transmission of the Service, including your User Files, may involve (a) transmissions over various networks; and (b) changes to conform and adapt to technical requirements of connecting networks or devices.
6. You must not upload, post, host, or transmit unsolicited email, or "spam" messages.
7. You must not transmit any worms or viruses or any code of a destructive nature.
8. If your bandwidth usage significantly exceeds the average bandwidth usage (as determined solely by Company) of other customers of the Service, we reserve the right to immediately disable your account until you can reduce your bandwidth consumption.

9. Company does not warrant that (i) the service will meet your specific requirements, (ii) the service will be uninterrupted, timely, or error-free, or (iii) any errors in the Service will be corrected.
10. You expressly understand and agree that Company shall not be liable for any direct, indirect, incidental, special, consequential or exemplary damages, including but not limited to, damages for loss of profits, goodwill, use, data or other intangible losses (even if Company has been advised of the possibility of such damages), resulting from: (i) the use or the inability to use the Service; (ii) the cost of procurement of substitute goods and services resulting from any goods, data, information or services purchased or obtained or messages received or transactions entered into through or from the Service; (iii) unauthorized access to or alteration of your transmissions or data; (iv) statements or conduct of any third party on the Service; (v) or any other matter relating to the Service.
11. The failure of Company to exercise or enforce any right or provision of the Terms of Service shall not constitute a waiver of such right or provision. The Terms of Service constitutes the entire agreement between you and Company and govern your use of the Service, superseding any prior agreements between you and Company (including, but not limited to, any prior versions of the Terms of Service).
12. Questions about the Terms of Service should be sent to support@zecter.com.

Cancellation and Termination

1. You are solely responsible for properly canceling your account. You may cancel your account by sending an email to support@zumodrive.com
2. All of your User Files will be deleted from the Service one month after cancellation. This information cannot be recovered once it has been deleted.
3. Company, in its sole discretion, has the right to suspend your account and refuse any and all current or future use of the Service, pending investigation, for any reason at any time. Such termination of the Service may result in the deactivation or deletion of your Account or your access to your Account, and the forfeiture and relinquishment of all User File in your Account. Company reserves the right to refuse service to anyone for any reason at any time.

Modifications to the Service and Prices

1. Company reserves the right at any time and from time to time to modify or discontinue, temporarily or permanently, the Service (or any part thereof) with or without notice.
2. Prices of all Services, including but not limited to free beta programs and monthly subscription plan fees to the Service, are subject to change upon 30 days notice from us. Such notice may be provided at any time by posting the changes our web site (http://www.zumodrive.com/) or the Service itself.
3. Company shall not be liable to you or to any third party for any modification, price change, suspension or discontinuance of the Service.

ANNEX 21 Norton online backup – Terms of Service[272]

Terms of service agreement

8. [...] In order to optimize the Software and Service Symantec may, at its discretion and without notice, add, modify or remove features from the Software or Service at any time. In such event, You may be required to upgrade to the latest version of the Software in order for the Service to continue to function correctly. You agree that Symantec may, in its sole discretion and from time to time, establish or amend general operating practices to maximize the operation and availability of the Service and to prevent abuses.

9. Privacy; Data Protection.
From time to time, depending on the settings for the Service, the Software and Service will collect certain information from You and the end users who use the computer on which the Software is installed (collectively, the "End Users"). The collected information is necessary for the purpose of delivering the functionality of the Software and Service and will be encrypted and transferred to Symantec so that it may be monitored by You; however, Symantec will not read such information or online communications. From time to time, the Software and Service may collect certain information from Your computer, which may include:

- Information regarding installation of the Software. This information indicates to Symantec whether installation of the Software was successfully completed and is collected by Symantec for the purpose of evaluating and improving Symantec's product installation success rate. This information will not be correlated with any personally identifiable information.
- The name given, during initial setup, to the computer on which the Software is being installed. If collected, the name will be used by Symantec as an account name for such computer under which You may elect to receive additional services and/or under which You may use certain features of the Software. You may change the account name at any time after installation of the Software (recommended).
- Other general, statistical information used for product administration and analysis, and for improving product functionality. This information will not be correlated with any personally identifiable information.

Symantec reserves the right to cooperate with any legal process and any law enforcement or other government inquiry related to your use of this Software. This means that Symantec may provide documents and information relevant to a court subpoena or to a law enforcement or other government investigation. In order to promote awareness, detection and prevention of Internet security risks, Symantec may share certain anonymous security information with research organizations and other security software vendors. Symantec may also use statistics derived from the information to track and publish reports on security risk trends. By using the Service, You acknowledge and agree that Symantec may collect, transmit, store, disclose and analyze such information for these purposes.

In addition, any Data that You transmit or store through the Service may be transferred to the Symantec group in the United States or other countries that have less protective data protection laws than the region in which You are situated (including outside the European Economic Area),

[272] http://www.Symantec.com/content/en/us/about/media/NOBU_TOS_21_USE.pdf

but Symantec has taken steps so that the Data, if transferred, receives an adequate level of protection, including by using data transfer agreements where required. If You have any questions about how Your Data is being handled, please contact Symantec Customer Service using the contact details in Section 16.

Symantec has no obligation to monitor use of the Service and/or Data transmitted or stored through the Service. To the maximum extent permissible under applicable law and notwithstanding the provisions of the fourth paragraph of article 9, Symantec reserves the right at all times to monitor, review, retain and/or disclose any Data or other information as necessary to satisfy any applicable law, regulation, legal process or governmental request, or to investigate any suspected breach of these Terms and Condition.

10. DISCLAIMER OF WARRANTY.

To the maximum extent permissible under applicable law, the software and service and any third party software or service are provided on an "as is" and "as available" basis, with all faults. Symantec and its licensors provide the service without warranties of any kind, written or oral, statutory, either express or implied, including without limitation, warranties of title, noninfringement, merchantability, fitness for a particular purpose, including those arising from course of dealing or course of trade and disclaims any such warranties. Symantec and its licensors do not warrant that the service or software will be uninterrupted, error-free, or secure. No advice or information given by Symantec, its licensors, affiliates, its agents, or its contractors or their respective employees will vary the terms of this agreement or create any warranty. Symantec is not responsible for defacement, misuse, abuse, neglect, improper use of the services by you, force majeure events such as improper electrical voltages or current, repairs, alterations, modifications by others, accidents, fire, flood, vandalism, acts of god, or the elements. To the maximum extent permissible under applicable law, Symantec technical support is not warranted and is used at your own risk. Symantec and its licensors make no warranty regarding transactions executed and content and information accessed by using the service. to the extent that any limitation in this section is not permitted by applicable law, such limitation will not apply to you to the extent it is barred by applicable law.

11. LIMITATION OF LIABILITY.

Some states and jurisdictions including member countries of the European economic area, do not allow for the limitation or exclusion of liability for incidental or consequential damages so the below limitation or exclusion may not apply to you.

- (a)To the maximum extent permissible under applicable law, you assume total responsibility for use and results of use of the service. Symantec and its licensors exercise no control over and disclaim any responsibility for the content or data created or accessible using the service. You agree not to use the service in high risk activities where an error could cause damage or injury.
- (b) To the maximum extent permissible under applicable law, regardless of the legal theory under which liability is asserted and regardless of whether Symantec has been advised of the possibility of liability, loss or damage, Symantec, its licensors, affiliates, agents, and contractors will not be liable to you for any incidental, indirect, special, reliance, punitive or consequential damages of any kind (including, without limitation, any loss of use, loss of business, lost or imputed profits or revenues, loss or destruction of content, information or data, costs of cover, interrupted service, or reliance upon the software and/or associated documentation) arising out of or related to this agreement, service or software.
- (c) To the maximum extent permissible under applicable law, with regard to any service related claim for damages that is not limited by this section, your exclusive remedies for such claim will be limited to the total charges paid by you to Symantec for the affected

service in the one month immediately preceding the occurrence of the event giving rise to the claim. Symantec's total aggregate liability arising from or related to this agreement will not exceed the total charges paid by you to Symantec under this agreement in the one month immediately preceding the occurrence of the event giving rise to the claim ("DAMAGE CAP").

- (d) Symantec and its licensors disclaim all liability or responsibility if service changes require changes to your equipment, degrade your equipment performance or service performance with the equipment, or make your equipment obsolete

16. GENERAL TERMS.

This Agreement will be governed by and construed under the laws of the State of California, without giving effect to such state's conflict of laws principles. Any legal action or proceeding related to this Agreement shall be instituted in a state or federal court in Santa Clara County, California. Symantec and You agree to submit to the jurisdiction of, and agree that venue is proper in, these courts in any such legal action or proceeding. If any provision of this Agreement is ruled invalid, such invalidity shall not affect the validity of the remaining portions of this Agreement. No amendment to this Agreement will be binding unless evidenced by a writing signed by the party against whom it is sought to be enforced. No waiver by either Symantec or You of any breach or default under this Agreement shall be deemed to be a waiver of any of any other breach or default under this Agreement. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A. or visit the Support page at www.Symantec.com.

17. Legal Effect.

This Agreement describes certain legal rights. You may have other rights under the laws of Your state or country. You may also have rights with respect to the party from whom You acquired the Software. This Agreement does not change Your rights or obligations under the laws of Your state or country if the laws of Your state or country do not permit it to do so.