January 13, 2010

Office of the Secretary
Federal Trade Commission
Room H-135 (Annex P2)
600 Pennsylvania Avenue, N.W.
Washington, DC 20580

Re: Comments of Rackspace Hosting, Inc. – Privacy Roundtables Project No. P095416

Dear Sir/Madam:

Rackspace Hosting, Inc. ("Rackspace") respectfully submits these comments in connection with the Commission's planned second Privacy Roundtable. Rackspace is a publicly traded company headquartered in San Antonio, Texas. We provide hosted information technology services including managed hosting, cloud computing, and email and apps, to over 80,000 business customers worldwide. We manage over 54,000 servers in our data centers.

The Commission has requested comments regarding the role of cloud computing services in addressing Internet-related privacy concerns. The term "cloud computing" is used in widely varying ways, so as an initial matter, we suggest that some clarity be given to this term for the purpose of this discussion. We note the comments of AT&T submitted in connection with the Second Roundtable [1], in which Mr. Bruce Byrd describes cloud computing as a business model under which the provision of data storage, compute capacity, and related functions are performed by a network operator inside a network, rather than by end users inside their customer premises. This is part of cloud computing model, but as Mr. Byrd states, this business model has existed for many years. The innovation that has given rise to the term "cloud computing" is a utility pricing model which allows users to pay for the computing resources they actually use, rather than paying for a dedicated computing resource which may not be fully used except at certain peak use times. This business model has been made possible by advances in computer virtualization technology, which allows the resources of a single physical computing device to be divided into distinct "virtual machines" that use a portion of the physical host's resources. A "cloud computing" provider links many physical machines, each running multiple virtual machines, to form a "cloud" of compute capacity. This "cloud" is thereby able to rapidly move and deploy the virtual machines among physical hosts to adjust to fluctuating demands on compute resources by its users, and maximize the overall use of the physical devices. At scale, this model dramatically lowers the cost of providing computing resources over traditional dedicated resource computing, which drives lower pricing, which in turn drives increased use of third party, off site providers.

[1] Comments of AT&T, Inc. submitted in connection with second roundtable, dated December 21, 2009.

In reviewing the materials and comments that have been provided to date, we note that there does not seem to be a careful consideration of the role of pure computing resource providers like Rackspace. Rackspace hosts data-rich applications for thousands of customers, both in its traditional dedicated hosting division and its newer cloud computing division. However, Rackspace plays no role in the collection or management of the data that it hosts for its customers[2]. Rackspace's customers conduct all of the activities related to revisions, updates, deletions and other tasks with respect to individual records within a database. The customers, and not Rackspace, are in a position to implement data privacy standards and technologies.

The failure to distinguish pure computing resource providers from "data processors" (those providers who do play a role in the management of databases at an individual data record basis) is a weakness in various existing regulatory schemes that were designed to protect personal data. This confusion results in less effective protection of the actual data, as the data managers believe that their regulatory requirements are met by the third party compute provider, who in fact does not even have notice, in most cases, of the type of data that is being hosted on its platform. [3] By analogy, the role of cloud computing providers is like that of other "utilities" such as an electric company, or water system. The utility provider does not have a role in determining how its customers use those resources, only in providing them.

Cloud computing providers do play a role in data security, which is a component of privacy protection. The security features of a cloud platform are uniform for all users. It is appropriate for cloud providers to fully disclose the security features of its platform, so that the potential users can evaluate whether the level and type of security is appropriate to the type of data that will be stored there. A cloud provider may elect to offer a relatively less secure, but lower priced, platform and this platform may be perfectly suited to certain types of non-sensitive data (public facing web content) but not sensitive data, such as health or financial data. Cloud users should have the information they need to determine if the platform is suitable for their business purposes.

---

[2] In certain instances, Rackspace may manipulate data or data applications, but only on the specific and detailed request of a customer as part of providing support to the customer in connection with the computing platform.

[3] For example, the HIPAA regulations require health care providers to obtain assurances from third parties who are given possession of covered data that they will use appropriate measures to safeguard the data. This is a sensible requirement where the business associate is assigned security decision making rights by the health care provider. However, this requirement is very often misunderstood in the context of a computing resources relationship, where the security decisions are made by the customer, based on the customer's budget and business needs. A customer may elect not to pay the extra fees required to implement certain security elements (such as an application firewall), but may insist that Rackspace sign an agreement representing that Rackspace will use appropriate measures to safeguard the data. Presumably the customer relies on having this agreement in place to satisfy its obligation to protect the data, in lieu of implementing the actual technical measures that would in fact provide meaningful protection.

In summary, any regulatory scheme implementing privacy safeguards should clearly delineate responsibility consistent with the level of control over the means by which it is stored and processed. Computing resource providers should be exempt from any requirement, other than to provide the specific infrastructure features that the data manager has contracted for.

Rackspace welcomes additional dialogue on these issues.

Respectfully Submitted,

Alice L. King
Associate General Counsel