PROSKAUER ROSE LLP

A Moment of Privacy

A newsletter brought to you by the Privacy and Data Security Practice Group at Proskauer Rose

NOVEMBER 2008

Edited by

Kristen J. Mathews

Welcome to "A Moment of Privacy," a newsletter brought to you by the Privacy and Data Security Practice Group at Proskauer Rose LLP.

"A Moment of Privacy" addresses one legal development each month in the area of privacy and data security law. We answer the questions our clients are asking, in a way that we hope gives practical information to our readers. If you send us your question, you may find your answer in an upcoming newsletter.

And now for this month's question:

Q: My company may begin using cloud computing in its IT infrastructure. Are there any privacy issues that I should be aware of?

For this question, we called in one of our international data transport experts, Jeremy Mittman, in Proskauer Rose's Privacy and Data Security Practice Group.

A: While the value of cloud computing certainly holds much promise, companies wishing to make the leap into the cloud would be well advised to consider the potential privacy issues.

Cloud computing, in its essence, is the migration or outsourcing of computing, hardware and storage functions to a third-party service provider, which hosts applications on the Internet through linked servers located worldwide. Cloud computing has captured the attention of IT professionals because it offers the appealing option of reducing a company's computer infrastructure and placing it in the hands of a vendor who can perform a company's computing needs more cheaply and efficiently than the company can itself.

The very newness of cloud computing means that its privacy implications have only begun to be addressed, but one can be sure that as cloud computing becomes more commonplace, countervailing privacy obligations are sure to collide with this innovative concept. Any company transferring its computing activities to the "cloud" risks running afoul of countries' laws governing data protection, most notably in the European Union, which arguably has the world's most stringent data protection laws.

In converting to cloud computing, companies are essentially handing over their data to third-party application service providers, who store and process such data in the "cloud," which could be anywhere in the world—usually, a company computing in the cloud does not know at any given time in what country its data resides. For example, instead of its data being stored on the company's servers, data is stored on the service provider's servers, which could be in Europe, in China, or anywhere else. This central tenant of cloud computing conflicts with the EU's requirements that a company know where the personal data in its possession is being transferred to at all times. As a result, cloud computing poses special problems for multinationals with EU employees or customers, such as:

- The EU Data Protection Directive places restrictions on the transfer of personal data from Europe to nations (such as the U.S.) whose data protection laws are not judged "adequate" by EU standards. As a result, using cloud computing (in which, for efficiency, data may be housed on servers worldwide), could run afoul of EU data protection law unless measures are taken to bring the international data exports into compliance with European law.

- The U.S. Safe Harbor Program — perhaps the most common means of compliance with EU requirements imposed when transferring the personal data of EU citizens to the US — may not satisfy a multinational's EU legal obligations, because, in cloud computing, data could be stored on servers outside of both Europe and the U.S, making the Safe Harbor Program ineffective.

- The use of Binding Corporate Rules — the newest method of EU international data transfer compliance — used alone also may be insufficient, because, in cloud computing, personal data will be transferred outside of the corporate "group" that is bound by the corporate rules.

- International data transfer issues aside, companies also will need to consider other privacy concerns when computing in the cloud, such as the possibility that data stored with another entity may be subject to subpoena and disclosed to the government of the jurisdiction where the cloud servers are located, perhaps without the company's permission or knowledge.

Of course, one way to comply with the EU Data Directive would be to ensure that EU personal data does not leave Europe in the first place. In fact, one cloud computing application service provider offers its customers the option to store their data only on European servers (for a higher fee, naturally). However, that will be an impractical solution as it will limit the very flexibility and efficiency that cloud computing was designed to provide.

This brief analysis is not to suggest that all instances of cloud computing are per se unlawful under European law. However, the very qualities of cloud computing that make it so intriguing and useful as an alternative to standard computing configurations are also the same aspects that raise data protection concerns. Given the enormous potential and benefits

of computing in the cloud, it seems that, once again, the law needs to catch up to technology.

Have a question? E-mail Kristen J. Mathews at kmathews@proskauer.com.

Privacy and Data Security Practice

Our Privacy and Data Security Practice is an outgrowth of our Internet, intellectual property, technology media & communications, labor and employment, health law, First Amendment, international law and litigation practices. Indicative of our experience and reputation in this relatively new field of law is the fact that the venerable Practising Law Institute (PLI) asked our Firm to create its first-ever treatise on the subject of privacy and data security law, called "Proskauer on Privacy," which was published in late 2006.

Privacy and Data Security Practice Group Partners:

Christopher Wolf, Chair
202.416.6818 – cwolf@proskauer.com

Tanya L. Forsheit
310.284.4508 – tforsheit@proskauer.com

Grégoire Goussu
33.1.53.05.60.11 – ggoussu@proskauer.com

Kristen J. Mathews
212.969.3265 – kmathews@proskauer.com

Jeffrey D. Neuburger
212.969.3075 – jneuburger@proskauer.com