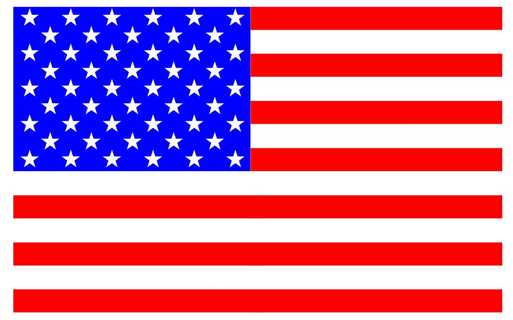
CERIAS

The Center for Education and Research in Information Assurance and Security

International Legal Implications for Cloud Computing

by Mary Horner

Advisor Dr. Sam Liles



“Access to personal data for national security and law enforcement purposes: It is of the utmost important to add to the future Regulation that controllers operating the in the EU must be prohibited from disclosing personal data to a third country if so requested by a third country’s judicial or administrative authority, unless this is expressly authorized by an international agreement or provided for by mutual legal assistance treaties or approved by a supervisory authority.” (1)

Privacy Protection in Europe

Article 8 of the European Convention on Human Rights (ECHR) of the Council of Europe

•Everyone has the right to respect for his private and family life, his home and his correspondence.

•There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

This protects the rights to respect for private life and the right to respect for correspondence, regardless of citizenship, origin, or place of residence.

Citizens have the right to find out about privacy infringements and the ability to defend themselves from government access.

“The United States takes the position that it can use its own legal mechanisms to request data from any Cloud server located anywhere around the world so long as the Cloud service provider is subject to U.S. jurisdiction: that is, when the entity is based in the United States, has a subsidiary or office in the United States, or otherwise conducts continuous and systematic business in the United States.” (2)

U.S. authorities have the power to request information from cloud providers for a criminal investigation. Jurisdiction under US law would be necessary, but this could be effected if a cloud provider does business in the US. One researcher states that it is a misconception that US jurisdiction only applies if the data is physically located in the United States.

Fourth Amendment

This covers situations in which a person has “a reasonable expectation of privacy” however this protection may be limited by the “Third Party doctrine”. Some researchers view this as problematic in the cloud environment since the transferal of data is inherent in the use of the cloud. Under this doctrine, do individuals relinquish their protections if they transfer data to a third party?

Selected References

1. Article 29 Data Protection Working Party., (2012 July, 1). *Opinion 05/2012 on Cloud Computing*, 01037/12/EN, WP 196. Retrieved from http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

2. Maxwell, W & Wolf, C., (2012 May, 23). A Global Reality: Governmental Access to Data in the Cloud, *A Hogan Lovells White Paper*. Retrieved from http://cryptome.org/2012/07/gov-spy-cloud.pdf

3, Van Hoboken, J.V.J, Arnbak, A.M, & van Eijk, N.A.N.M., (2012 November). Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act, *Institute for Information Law*, University of Amsterdam. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2181534

CERIAS

PURDUE UNIVERSITY