



Attorneys:

- **Timothy G. Ronan**
tronan@pullcom.com
203.674.7933

CYBER LAW TRACKER: April 2010

The Latest in Cybersecurity and Infrastructure Protection Legal Developments

CLOUD SECURITY ALLIANCE RELEASES WHITE PAPERS ON CLOUD COMPUTING SECURITY THREATS AND RISK MITIGATION

Posted on April 21, 2010, by Timothy G. Ronan

There is no doubt that cloud computing constitutes a paradigm shift in information technology management. As with any new technology, users and potential users are excited by the benefits it offers, but concerned about the risks of cloud computing, particularly if not properly secured.

The Cloud Security Alliance (CSA) has released two white papers outlining the top threats posed by cloud computing and one offering security guidance for critical areas of focus in cloud computing. Among the threats identified by CSA are fraudulently motivated providers of cloud computing services, insecure software interfaces, the possibility of malicious insider abuse and the threat of data loss or leakage. These threats apply equally to the three cloud computing models: infrastructure as a service, platform as a service and software as a service. In its security guidance white paper, CSA offers a rather comprehensive set of recommendations on how to mitigate the risks attendant to a transition to cloud computing to make that transition as secure as possible with, among other things, recommendations for a secure architectural framework, disaster recovery protocols, application security and encryption and key management.

pullcom.com  @pullmancomley

BRIDGEPORT | **HARTFORD** | **SPRINGFIELD** | **WAKEFIELD** | **WATERBURY** | **WESTPORT** | **WHITE PLAINS**
203.330.2000 | 860.424.4300 | 413.314.6160 | 401.360.1533 | 203.573.9700 | 203.254.5000 | 914.705.5355

CYBER LAW TRACKER: April 2010

For more on this subject, you should visit the CSA website at <http://www.cloudsecurityalliance.org>. The CSA is a nonprofit organization led by a coalition of industry practitioners, corporations, associations and other key stakeholders to promote best practices for providing security assurance within cloud computing and “to provide education on the uses of cloud computing to help secure all other forms of computing.”

NSA SUSPENDS METADATA COLLECTION

Posted on April 19, 2010, by T. Scott Cowperthwait

Metadata is a household term in business litigation. In the early stages of a business dispute, preservation letters are regularly sent to the opposing party and/or third parties which may possess electronically stored information that has been identified as an important source of discovery and evidence in the dispute. These data collection efforts can turn a case.

The collection and analysis of metadata also has become a common and important intelligence gathering tool utilized by the National Security Agency (NSA), the federal intelligence agency which is jointly tasked with gathering electronic information that America’s adversaries wish to keep secret and protecting America’s vital national security information and systems from theft or damage by others. The Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1801, et seq., regulates electronic surveillance and the gathering of related evidence for intelligence purposes, and the Foreign Intelligence Surveillance Court (FISA Court) grants orders to intelligence agencies like the NSA to monitor U.S. citizens and residents in terrorism and espionage cases. Recently, the FISA Court reviewed the process relating to the NSA's collection of certain types of electronic data, the metadata of which includes the origin, destination and path of an e-mail, the phone numbers called from a particular telephone, and the Internet address associated with Internet phone calls. As a result of this review, the NSA has suspended its metadata collection practice, leaving intelligence officials and members of Congress concerned that important electronic data may not be captured. NSA officials and members of U.S. congressional intelligence committees are attempting to remedy the FISA Court’s concerns, which ultimately would lead to the return of the NSA’s electronic data collection efforts.

This publication is intended for educational and informational purposes only. Readers are advised to seek appropriate professional consultation before acting on any matters in this update. This report may be considered attorney advertising. To be removed from our mailing list, please email unsubscribe@pullcom.com with "Unsubscribe" in the subject line. Prior results do not guarantee a similar outcome.