Legal Clouds: How to Balance Privacy with Legitimate Surveillance and Lawful Data Access

Submission deadline: 1 March 2015 • Publication date: July/August 2015

With the increasing popularity of cloud services and their potential to either be the target of or the tool used in a cybercrime activity, organizational cloud service users need to ensure that their (cloud) data is secure, and in the event of a compromise, they must have the capability to collect evidential data.

Surveillance of citizens by their governments is not new. The relatively recent revelations of Edward Snowden (former NSA contractor) of the extensive surveillance (including of cloud service providers and users) by NSA, however, reminded us of the need to balance a secure cloud computing system with the rights of individuals to privacy. This is further complicated by the need to protect the community from serious and organized crimes, terrorism, cyber-crime, and other threats to national security interests. This presents serious implications for the ability of governments to protect their citizens against cyber security threats. It remains an under-researched area due to the interdisciplinary challenges specific to this field.

This special issue will focus on cutting edge research from both academia and industry on the topic of balancing cloud user privacy with legitimate surveillance and lawful data access, with a particular focus on cross-disciplinary research. For example, how can we design technologies that will enhance "guardianship" and the "deterrent" effect in cloud security at the same time as reducing the "motivations" of cybercriminals?

Topics of interest include but are not limited to:

- Advanced cloud security
- Cloud forensics and anti-forensics
- Cloud incident response
- Cloud information leakage detection and prevention
- Enhancing and/or preserving cloud privacy
- Cloud surveillance
- Crime prevention strategies
- Legal issues relating to surveillance
- Enhancing privacy technology for cloud-based apps
- High quality survey papers on the above topics are welcome.

Special Issue Guest Editors

Kim-Kwang Raymond Choo, University of South Australia

Rick Sarre, University of South Australia

Submission Information

Submissions will be subject to *IEEE Cloud Computing* magazine's peer-review process. Articles should be at most 6,000 words, with a maximum of 15 references, and should be understandable to a broad audience of people interested in cloud computing, big data, and related application areas. The writing style should be down to earth, practical, and original.

All accepted articles will be edited according to the IEEE Computer Society style guide. Submit your papers through Manuscript Central at https://mc.manuscriptcentral.com/ccm-cs. Contact the guest editors at ccm4-2015@computer.org.

www.computer.org/cloudcomputing