

CALL FOR PAPERS
IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY
Special Issue on Privacy and Trust Management in Cloud and Distributed Systems

Guest Editors

<i>Karl Aberer,</i>	École Polytechnique Fédérale de Lausanne, Switzerland (karl.aberer@epfl.ch)
<i>Sen-ching Samson Cheung,</i>	University of Kentucky, USA (cheung@engr.uky.edu)
<i>Jayant Haritsa</i>	Indian Institute of Science, India (jharitsa@gmail.com)
<i>Bill Horne</i>	Hewlett-Packard Laboratories, USA (william.horne@hp.com)
<i>Kai Hwang</i>	University of Southern California, USA (kaihwang@usc.edu)
<i>Yan (Lindsay) Sun</i>	University of Rhode Island, USA (yansun@ele.uri.edu)

With the increasing drive towards availability of data and services anytime anywhere, **privacy** risks have significantly increased. Unauthorized disclosure, modification, usage, or uncontrolled access to privacy-sensitive data may result in high human and financial costs. In the distributed computing environments, **trust** plays a crucial role in mitigating the privacy risk by guaranteeing meaningful interactions, data sharing, and communications. Trust management is a key enabling technology for security and privacy enhancement. While privacy preservation and trust management are already challenging problems, it is imperative to explore how privacy-oriented and trust-oriented approaches can integrate to bring new solutions in safeguarding information sharing and protecting critical cyber infrastructure. Furthermore, there are questions about whether existing trust models and privacy preserving schemes are robust against attacks. This Call for Papers invites researchers to contribute original articles that cover a broad range of topics related to privacy preservation and trust management in cloud and distributed systems, with a focus on emerging networking contexts such as social media, cloud computing, and power grid systems.

Example topics include but are not limited to

- *Privacy Enhanced Technology*: privacy preserving data mining, publishing, and disclosure; access control, anonymity, audit, and authentication; applied cryptography, cryptanalysis, and digital signatures in PET; abuse cases and threat modeling; theoretical models and formal methods; application of physical security for privacy enhancement.
- *Trust and Reputation Management*: trust management architectures and trust models; quantitative metrics and computation; security of trust management protocols/systems; evaluation and test bed; trust related privacy enhancement solutions.
- *Privacy and Trust in Emerging Complex Systems* including: social networking; cloud computing; power grid systems; sensor networks; Internet of Things; multimedia surveillance networks.
- *Other Related Topics* such as trust and privacy policies; human factors and usability; censorship; economics of trust and privacy; behavior modeling.

Submission Procedure: Manuscripts are to be submitted according to the Information for Authors at <http://www.signalprocessingsociety.org/publications/periodicals/forensics/forensics-authors-info/> using the IEEE online manuscript system, Manuscript Central. Papers must not have appeared or be under review elsewhere.

Schedule

Submission deadline:	June 11, 2012
First Review:	September 12, 2012
Revisions Due:	October 31, 2012
Final Decision:	January 15, 2013
Final manuscript due:	February 20, 2013
Tentative publication date:	June 1, 2013