Security and Communication Networks

Special Issue on
Privacy Implications of the Smart Environment in the 21st Century

WILEY | Hindawi

CALL FOR PAPERS

We live in the *smart environment* where devices are interconnected and interact with each other autonomously. For example, Internet of Things (IoT) and smart home networks monitor users' daily activities and behavior and adjust the smart sensors/devices to create the seamless environment without involving their input. As another example, semiautonomous and autonomous driving environment will continuously monitor the driver's behavior as well as the surrounding environment to make the appropriate safety decisions with minimal driver involvement. However, creating such seamless environments is data driven; the *monitoring* aspect involves collecting user data to build personalized profiles, and the ownership of such data is unclear. Are the data owners in control of their own data? Do they even know precisely what data is being collected and how it is being used?

Oftentimes, users consent to let the sensors and devices collect potentially sensitive information, but such consent is meaningless from user's privacy perspective; they may be forced to agree to experience the advanced technologies possibly at a reduced cost. To certain degree, the technology advancement seems to be altering the definition of privacy, and the big question is how we can inform users about the privacy implications effectively and efficiently without overloading their cognition.

This special issue looks for innovative approaches that tackle the challenge in finding the balance between the advanced technologies and their privacy implications in the smart environments (e.g., smart homes/cities, vehicular networks). In particular, we are interested in cross-disciplinary research that addresses legal and user aspects to practically achieve privacy and anonymity in the smart environment. As each smart environment has distinct characteristics, different privacy concerns exist by nature. Hence, a submission should clearly state which environment it is addressing.

Potential topics include but are not limited to the following:

- Large-scale measurements or in-depth case studies of privacy violation (e.g., smart devices secretly sending data back to foreign countries)
- Anonymization and deanonymization techniques for monitored data in the smart environment
- Techniques to detect or circumvent interception (e.g., using censors or middleboxes) in the smart environment
- Novel side-channel attacks and mitigation techniques for the smart environment
- Practical mechanisms for balancing accountability and anonymity in the smart environment
- End-user privacy, data providers privacy, and application platform privacy for the smart environment
- Legal and regulatory implications and proposals on lawful interception (e.g., impact of EU's General Data Protection Regulation on the design and implementation of smart devices)
- User-centric privacy solutions (e.g., automatic extraction of privacy policies for violation checking, interface that helps users understand privacy policies, etc.)

Authors can submit their manuscripts through the Manuscript Tracking System at https://mts.hindawi.com/submit/journals/scn/pisec/.

Papers are published upon acceptance, regardless of the Special Issue publication date.

Lead Guest Editor
Tiffany H. Kim, HRL Laboratories, Malibu, USA
hyunjin@cmu.edu

Guest Editors
Hsu-Chun Hsiao, National Taiwan University, Taipei, Taiwan
hchsiao@csie.ntu.edu.tw

Yue-Hsun Lin, JD.COM R&D Center, Santa Clara, USA
tenma.lin@gmail.com

Submission Deadline
Friday, 8 June 2018

Publication Date
October 2018