PACIS 2022 Track: Cybersecurity, Privacy, and Ethical Issues

Track Description

Recent technological advancements such as analytics, artificial intelligence (AI), internet of things (IoT), social media, and big data are rapidly transforming our daily lives, businesses, and society at large. However, as our dependency on technologies is ever-increasing, we are also witnessing many unintended negative consequences related to the use of technologies, which sometimes exceed the positive utility gained from it. From cybersecurity perspectives, the proliferation of social media and mobile technologies intensifies the concerns of data breaches. Criminals are finding new ways online to conduct illegal activities like online fraud, identity theft, and cyber terrorism. As a result, firms are actively seeking solutions to address these cybersecurity and privacy issues, and governments are implementing security and privacy policies. More recently, we see the emergence of undesirable ethical issues in the use of technologies. As exemplified by the case of Cambridge Analytica and Facebook, improper use of consumer data has serious business implications with possible legal, social, and political consequences. Online platforms are also criticized for some major failures such as the spread of fake news and the reinforcement of echo chambers, resulting in political polarization.

As a response to these challenges, this track seeks academic contributions that attempt to provide a better understanding of (1) the potential security, privacy, and ethical issues in the use of technologies; (2) consequences of these issues on individuals, businesses, and society; (3) possible solutions to address the concerns of security, privacy, and ethical issues while realizing the values generated by the technologies. Submitted manuscripts can draw on any theoretical backgrounds and methodological approaches.

Topics of interest include, but are not limited to:

- Data security and breaches
- User privacy and confidentiality
- Ethical use of data and analytics
- Internet-enabled crimes
- Ethically undesirable online practices
- Information security policy and compliance
- Business, legal, social, political consequences of IS security and privacy
- The dark web, live-streaming of crimes, harmful online content, etc.
- Surveillance and its impact on security, privacy and ethics in organizations
- Fake news, online discrimination
- Possible solutions, regulations, policies
- Tradeoffs between analytics initiatives and security/privacy concerns
- Security and privacy issues on emerging technologies such as AI applications, blockchain technologies, IoT, etc.)
- Security threat intelligence
- Security/privacy concerns on crowdsourcing/crowdfunding platforms

Important Dates
Paper Submission Deadline: March 1, 2022
Paper Decision Notification: Before May 1, 2022
Camera-Ready Due: June 1, 2022

Track Chairs
Seung Hyun Kim (seungkim@yonsei.ac.kr), Yonsei University, Korea
Gene Moo Lee (gene.lee@sauder.ubc.ca), University of British Columbia, Canada
Dan J. Kim (Dan.Kim@unt.edu), University of North Texas, USA

Associate Editors
Arslan Aziz, University of British Columbia
Donghyuk Shin, Arizona State University
Alvin Leung, City University of Hong Kong
Vincent Zhuang, City University of Hong Kong
Shu He, University of Connecticut
Arion Cheong, California State Polytechnic University, Pomona
Yulia Sullivan, Baylor University
Kai Li, Nankai University
Tom Mattson, University of Richmond
Mehrdad Koohikamali, California State Polytechnic University, Pomona
Andrew Harrison, University of Cincinnati
Hwee-Joo Kam, University of Tampa
Jiye Baek, Korea University
Mike Yoon Han, Harbin Institute Of Technology
Jinseon Choe, Yonsei University
Jungkook An, Sun Moon University
Byungwan Koh, Korea University