Pervasive Surveillance and Privacy

Florian Schaub, *University of Michigan, Ann Arbor, MI, 48103, USA*
Junehwa Song, *Korea Advanced Institute of Science and Technology, Daejeon, 34141, South Korea*
Yaxing Yao, *University of Maryland Baltimore County, Baltimore, MD, 21250, USA*

Pervasive computing is flourishing; smart sensors and actuators have found their way into every corner of our daily lives. They are deftly interwoven with each other and their context, making environments ever more intelligent and convenient for users. Sensor-enabled surveillance systems are providing an additional layer of safety to our homes and our cities. Internet-connected appliances are automating routine tasks in smart homes to make our lives more convenient. Wearable devices are keeping track of minute details of our behaviors and activities to improve our health conditions. Augmented and virtual reality technologies are assisting people with disabilities to support their cognitive or physical capacity. However, these improvements and benefits come with potential costs to our privacy. Pervasive surveillance, even when carefully crafted, designed, and deployed, could lead to a severe invasion of our liberty, autonomy, and well-being. Such invasions could occur, for instance, due to government surveillance in the interest of increasing public safety, workplace surveillance to improve efficiency or employee well-being, consumer surveillance by companies for the sake of profit increase, and also family surveillance by intimate partners and family members.

The aim of this special issue is to discuss pervasive surveillance and privacy risks, surveillance detection approaches, surveillance and counterveillance, and privacy-enhancing approaches to thwart surveillance attempts. The accepted papers address a variety of topics, ranging from privacy preserving technologies to literature reviews to identify promising research directions.

In [A1], Zuo and Sigg focus on personalized gestures to enhance privacy protection and safety for gesture-controlled pervasive objects (e.g., drones and smart TVs) through motion transfer. Their demonstration using RGB-video data shows promising outcomes.

In [A2], Wang et al. discuss a framework that introduces data obfuscation between audio sensors and recognition algorithms in audio-based applications. They highlight the key innovation that allows users to opt in to tasks they would like to protect.

In [A3], Lee and Lee discuss the concept of "dynamic consent," a type of informed consent that enables granular data consent and management with promise for pervasive computing and pervasive health applications, and conduct a scoping review of the dynamic consent literature to inform usable privacy consent design.

In [A4], Zuniga et al. present an innovative method for discovering covert surveillance devices using thermal imaging integrated with off-the-shelf consumer devices. Their extensive and systematic evaluation of the proposed method shows its effectiveness in identifying covert devices even after considering other factors, such as distance to other objects, luminosity of the space, and types of cameras.

The collection of research papers included in this special issue illustrates the wide range of directions in which pervasive computing technology can be further enhanced by various privacy protection techniques to reduce surveillance risks. We hope that you will enjoy this special issue as much as we have enjoyed preparing it.

APPENDIX RELATED ARTICLES

[A1] Zuo and Sigg, "Personalized gestures through motion transfer: Protecting privacy in pervasive surveillance," *IEEE Pervasive Comput.*, vol. 21, no. 4, pp. 8–16, Oct.–Dec. 2022, doi: 10.1109/MPRV.2022.3210156.

[A2] Wang et al., "An opt-in framework for privacy protection in audio-based applications," *IEEE Pervasive Comput.*, vol. 21, no. 4, pp. 17–24, Oct.–Dec. 2022, doi: 10.1109/MPRV.2022.3210377.

[A3] Lee and Lee, "Toward dynamic consent for privacy-aware pervasive health and well-being: A scoping review and research directions," *IEEE Pervasive Comput.*, vol. 21, no. 4, pp. 25–32, Oct.–Dec. 2022, doi: 10.1109/MPRV.2022.3210747.

1536-1268 © 2022 IEEE
Digital Object Identifier 10.1109/MPRV.2022.3210786
Date of current version 23 December 2022.

[A4] Zuniga et al., "See no evil: Discovering covert surveillance devices using thermal imaging," *IEEE Pervasive Comput.*, vol. 21, no. 4, pp. 33–43, Oct.–Dec. 2022, doi: 10.1109/MPRV.2022.3187464.

FLORIAN SCHAUB is an associate professor in the School of Information and in the College of Engineering, University of Michigan, Ann Arbor, MI, 48103, USA. Schaub received his Ph.D. degree in computer science from the University of Ulm, Ulm, Germany. Contact him at fschaub@umich.edu.

JUNEHWA SONG is a professor in the School of Computing and KAIST-endowed Chair Professor at the Korea Advanced Institute of Science and Technology, Daejeon, 34141, South Korea. Song received his Ph.D. degree in computer science from the University of Maryland at College Park, College Park, MD, USA. Contact him at junesong@kaist.ac.kr.

YAXING YAO is an assistant professor in the Department of Information Systems, University of Maryland Baltimore County, Baltimore, MD, 21250, USA. Yao received his Ph.D. degree in information science from Syracuse University, Syracuse, NY, USA. Contact him at yaxingyao@umbc.edu.