

# $\delta$ -Risk: Toward Context-aware Multi-objective Privacy Management in Connected Environments

KARAM BOU-CHAAYA and RICHARD CHBEIR, Universite de Pau et des Pays de l'Adour, E2S UPPA, LIUPPA, Anglet, France

MANSOUR NASER ALRAJA, Dhofar University, Oman

PHILIPPE ARNOULD, Universite de Pau et des Pays de l'Adour, E2S UPPA, LIUPPA, Mont-de-Marsan, France

CHARITH PERERA, Cardiff University, United Kingdom

MAHMOUD BARHAMGI and DJAMAL BENSLIMANE, Université Claude Bernard Lyon 1, LIRIS lab, France

In today's highly connected cyber-physical environments, users are becoming more and more concerned about their privacy and ask for more involvement in the control of their data. However, achieving effective involvement of users requires improving their privacy decision-making. This can be achieved by: (i) raising their awareness regarding the direct and indirect privacy risks they accept to take when sharing data with consumers; (ii) helping them in optimizing their privacy protection decisions to meet their privacy requirements while maximizing data utility. In this article, we address the second goal by proposing a user-centric multi-objective approach for context-aware privacy management in connected environments, denoted  $\delta$ -Risk. Our approach features a new privacy risk quantification model to dynamically calculate and select the best protection strategies for the user based on her preferences and contexts. Computed strategies are optimal in that they seek to closely satisfy user requirements and preferences while maximizing data utility and minimizing the cost of protection. We implemented our proposed approach and evaluated its performance and effectiveness in various scenarios. The results show that  $\delta$ -Risk delivers scalability and low-complexity in time and space. Besides, it handles privacy reasoning in real-time, making it able to support the user in various contexts, including ephemeral ones. It also provides the user with at least one best strategy per context.

CCS Concepts: • Security and privacy → Privacy-preserving protocols; • Theory of computation → Continuous optimization

Additional Key Words and Phrases: User-centric privacy, privacy risk quantification, privacy by design, context-aware computing, semantic reasoning, Internet of Things

This work is supported by the Research Council (TRC), Sultanate of Oman (Block Fund-Research Grant).

Authors' addresses: K. Bou-Chaaya and R. Chbeir, Universite de Pau et des Pays de l'Adour, E2S UPPA, LIUPPA, Anglet, France; emails: {karam.bou-chaaya, richard.chbeir}@univ-pau.fr; M. N. Alraja, Dhofar University, Salalah 2509, Oman; email: malraja@du.edu.om; P. Arnould, Universite de Pau et des Pays de l'Adour, E2S UPPA, LIUPPA, Mont-de-Marsan, France; email: philippe.arnould@univ-pau.fr; C. Perera, Cardiff University, United Kingdom; email: charith.perera@ieee.org; M. Barhamgi and D. Benslimane, Université Claude Bernard Lyon 1, LIRIS lab, Lyon, France; emails: {mahmoud.barhamgi, djamal.benslimane}@univ-lyon1.fr.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from [permissions@acm.org](mailto:permissions@acm.org).

© 2021 Association for Computing Machinery.

1533-5399/2021/05-ART51 \$15.00

<https://doi.org/10.1145/3418499>