RTG Privacy and Trust for Mobile Users

Stands for:

- ✓ Individual Doctoral Program
- ✓ Internationality and Interdisciplinarity
- ✓ Extensive Mentoring & Support
- ✓ Team Spirit & Family Friendliness
- ✓ PhD Life & Events
- ✓ DFG Financing

Fachbereich Informatik

CYSEC
Cybersecurity
TU Darmstadt

GOETHE
UNIVERSITÄT
FRANKFURT AM MAIN

UNIKASSEL
VERSITÄT

Interested to Join or Contact us?

As a member (Master student, PhD candidate, Post-doc) at the Doctoral College, you will be part of a young, innovative and interdisciplinary team. You will help users to protect their privacy and to make the Internet a more trustworthy place.

As a Mercator Fellow or Guest Researcher
We are proud to be one of the RTGs funded by DFG that is able to invite Mercator fellows and guest researchers. The stay of researchers from abroad fosters intense, long-term project-based collaboration between resident researchers of the RTG and foreign universities.

As a Stakeholder of Privacy or Trust
We are always keen to exchange and share insights with intersted accademics worldwide, with industry, press and politicians.

Contact:
koordination@privacy-trust.tu-darmstadt.de

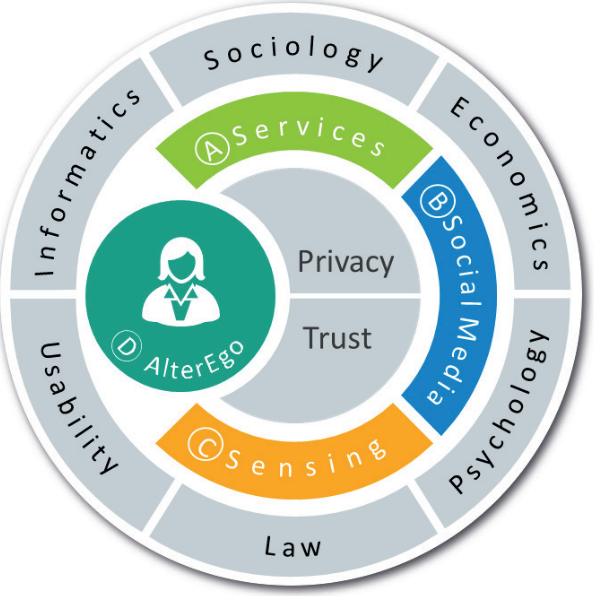
Privacy and Trust for Mobile Users

Interdisciplinary Doctoral College

TECHNISCHE
UNIVERSITÄT
DARMSTADT

DFG Deutsche Forschungsgemeinschaft
German Research Foundation

Interdisciplinary Doctoral College
Privacy and Trust for Mobile Users



Almost the entire world population utilizes mobile devices such as smartphones, handling more and more sensitive information. Users become increasingly exposed while services in the Internet become ever more opaque. Serious financial, legal and social consequences are impending from their deplorable trend.

The research training group aims to face these dangers by developing novel scientific concepts for user empowerment.

Research Area A:
Privacy and Trust in Service Networks

Fundamental Ideas

User empowerment is fostered by **technical** means, such as (i) metrics that help assessing and understanding privacy choices and their implications and (ii) novel privacy enhancing techniques. The application of 'interventions' becomes more effective with the **psychological** modelling of user decision processes and preferences. The development of privacy-friendly business models addresses the **economic** challenges of privacy and trust.

Resarch Area B:
Privacy and Trust in Social Networks

Fundamental Ideas

The **sociological** examination of trust in the sense of normative expectations of the society sheds a new light on the conflicting interpretations of privacy & trust, as well as institutial and regulatory implications of data protection. The combination of anonymous/privacy-preserving approaches and well-established social media **technologies** leads to hybrid solutions, maintaining the potential of data analytics and, therefore, balancing user and provider interests. The digitalization of social structures suggests the **socio-economical** quantification of social capital and its outcomes.

Research Area C:
Privacy and Trust in Sensor Augmented Environments

Fundamental Ideas

New transparency-enhancing and trust-establishing **technologies** allow users to regain control over the proliferation of sensor/IoT devices, both body-worn and encountered in our environment. From a **legal** perspective, sensor data may be impersonal at the time of capturing, but become person-related later in the context of (big) data analytics. This pecularity suggests the identification of risks and gaps in the current data protection **law** and proposes new cautionary measures to mitigate the consequences.

Research Area D:
Privacy and Trust via AlterEgo

Fundamental Ideas

User empowerment may be thwarted if vast amounts of privacy-related decisions are needed. This calls for **usability** approaches that learn from past decisions and consequences, reflect the trustworthiness of services, and suggest & automate decisions in the interest of the user. Key challenges are **socio-technically** designed mobile & personal devices that users can rely on as 'AlterEgos', i.e., proxies to the digital world. Their duty: to assess and establish trust, and negotiate consent in a privacy-preserving manner.