Call for Papers, Workshops, and Tutorials – 15th IFIP Summer School on Privacy and Identity Management

"It's complicated": Exploring the relationship between cybersecurity and privacy, and improving training and awareness

The 15th IFIP Summer School on Privacy and Identity Management (17-21 August 2020 in Brno, Czechia, `www.ifip-summerschool.org`) takes a *holistic approach to society and technology,* supporting interdisciplinary research exchange through keynote lectures, tutorials, workshops, and paper presentations.

In particular, we welcome *contributions combining any of the following perspectives:* anthropological, economic, ethical, historical, legal, media & communication, regulatory, sociological, surveillance, technical, philosophical, political, and psychological studies.

The IFIP Summer School encourages not only *interdisciplinarity* but also broader *diversity.* It particularly welcomes submissions on how to foster gender and cultural balance in cybersecurity research and policy, and notably tutorials and workshops about how to raise awareness in these matters.

Theme

Contributions dealing with the *complex relations between cybersecurity and privacy* are most welcome. These relations are manifest at both regulatory and practical levels: with digital media and information technology as everyday commodities, an increasing number of attacks on IT security are based on privacy breaches and privacy breaches are facilitated by security attacks. Examples include CEO fraud, spear fishing, and leakage of consumer information like credit card details. Although there is a general consensus that security, privacy, and data protection are interrelated, *the complexity of their relations has not yet been fully explored.* Key questions include: What are the intersections, i.e., conflicts, overlaps or compliance challenges, between the different regulatory frameworks (e.g., GDPR, NIS Directive, PSD2, and forthcoming ePrivacy Regulation) affecting these three fields? How do they relate to *technologies that protect ICT* and its users (e.g., cryptography that can provide confidentiality and anonymity)? How can privacy and security be co-engineered, satisfying all by-design paradigms? What *side-effects* occur during such co-design? What are the possible *societal consequences* regarding citizen (dis)empowerment, surveillance, and human rights? A special focus of this School is placed on *how to train and educate staff* at all levels in industries dependent on ICT, e.g., cyber ranges and other training methods, as well as how to train the trainers (including the role of Data Protection Officers) in these efforts.

Organization of research papers, workshops, and tutorials

The research paper presentations and the workshops focus on involving students, and on encouraging the publication of *high-quality, thorough research papers* by students and young researchers. To this end, the School offers a *three-phase review process* for submitted papers. In the first phase, submissions should be abstracts of a maximum of 2 pages. Submissions within the scope of the call are selected for presentation at the School. For accepted submissions, the full papers of up to 16 pages in length, in Springer LNCS format, are to be submitted before the Summer School, and will appear in the (unreviewed) pre-proceedings. Before the second review phase, students have time to revise their papers taking into account the discussion that took place at the Summer School. These revised, full papers are reviewed soon after the Summer School by Programme Committee members. Based on these reviews, papers might be accepted, conditionally accepted, or rejected. Accepted and (after satisfactory revision) conditionally accepted papers will be included in the Summer School's proceedings, which will be published by Springer.

Workshops are expected to last one or two hours and must *generate short papers* that recapitulate the outcome and the kinds of discussion raised in the School, for inclusion in the post-proceedings. Proposals should contain a *2-page statement* summarizing the topic(s) to be discussed and the expected contributions from the audience members, e.g. responding to a questionnaire or conducting a small experiment. Proposers should indicate whether any special equipment is needed for the workshop, such as audio-visual systems or computational equipment and support.

Tutorials are expected to last one or two hours. Proposals should contain a *2-page summary* and state the level and background required for audience members to follow the tutorial.

Topics include but are not limited to:

- Technical and Organizational Measures for Privacy and Security
  - 'by-design and default' mechanisms for: privacy, value-sensitivity, ethics, human rights, impact and risk assessments, data protection on the ground
  - data breach notification and its side effects
  - integration of privacy and security into agile development
  - privacy-enhancing technologies (PETs) and transparency-enhancing technologies (TETs)
  - privacy and identity management (services, technologies, infrastructures, usability aspects, legal and socio-economic aspects)
  - privacy and security in citizens' digital communications, online platforms, e-mail and instant messaging
  - usable privacy & security
- Metrics, Standards, Ethics and Norms
  - complementarity and friction between data subject rights, security, and privacy-by-design
  - interactions, i.e. compliance, overlaps and conflicts in challenges of cybersecurity and data protection norms (e.g., NIS directive, GDPR, PSD2, upcoming ePrivacy regulation)
  - privacy and security evaluation, metrics, certifications, certification mechanisms, auditing experiences, standards, and seals
  - privacy protection and, in particular, confidentiality of communications by both traditional players/incumbents and over the top media services
  - regulatory regimes and instruments, including ethical frameworks
- Training and Education for Privacy and Security
  - awareness-raising, digital literacy and data (infrastructure) literacy
  - research ethics and approvals
  - social accountability
  - training and education methodologies, cyber ranges
- Socio-technical perspectives on privacy and data protection
  - awareness, attitudes, skills and behaviour of citizens and organisations (including SMEs) regarding da-ta privacy, surveillance, and (cyber)security
  - integrative approaches for diversity (gender, accessibility, economics)
  - relation between privacy, public values and AI-based systems, and (global) consequences for policy and society
  - socio-cultural practices, perspectives and (dis)trust by users/employees regarding data-driven technologies and data capture and processing, in various spheres of life (health, smart cities, banking, media, education).

Why should I submit?

Accepted papers will receive thorough discussions during the School and provide students with an opportunity to be published in the IFIP AICT series by Springer. Students who present a paper can receive a course certificate awarding 3 ECTS points at the PhD level. Students whose papers are already at full submission length, and of sufficient quality for a PhD seminar thesis, can receive a course certificate awarding 6 ECTS points at the PhD level. The certificate can state the topic of the paper so as to demonstrate its relationship (or otherwise) to the student's master or PhD thesis. We encourage submissions from students from emerging economies: support is being applied to from the IFIP Digital Equity Fund to ease student travel. Last but not least, the summer School will take place in the beautiful city of Brno, a member of the UNESCO creative city network.

Important Dates

Abstracts Deadline:	1 May 2020 23:59(AoE)
Acceptance Decision:	Not later than 05 Jun 2020 (AoE)
Full Draft Paper:	10 Aug 2020 23:59(AoE)
Full Paper:	17 Sep 2020 23:59(AoE)
Reviews:	31 Oct 2020 (AoE)
Camera Ready:	30 Nov 2020 (AoE)