

Call for Contributions

Note: Onsite and Online Options

In order to accommodate a large number of situations, we are offering the option for either physical presence or virtual participation. We would be delighted if all authors manage to attend in person, but are aware that special circumstances are best handled by having flexible options.

1. **Inform the Chair:** with the Title of your Contribution

2. **Submission URL:**

<https://www.iariasubmit.org/conferences/submit/newcontribution.php?event=ICDS+2020+Special>

Please select Track Preference as **PPODS**

Special track

PPODS: Protecting Privacy in Open (& big) Data Settings

Chairs and Coordinators

Dr. Sunil Choenni, Professor at Rotterdam University of Applied Sciences, Research Center Creating 010,
Rotterdam, The Netherlands

Head of Statistical Data and Policy Analysis Division (SIBa), Research and Documentation Centre, Ministry of
Justice and Security, The Hague, The Netherlands

r.choenni@hr.nl

Dr. Mortaza S. Bargh, Professor at Rotterdam University of Applied Sciences, Research Center Creating 010,
Rotterdam, The Netherlands

Scientific Researcher at Statistical Data and Policy Analysis Division (SIBa), Research and Documentation
Centre, Ministry of Justice and Security, The Hague, The Netherlands

m.shoae.bargh@hr.nl

along with

ICDS 2020, The Fourteenth International Conference on Digital Society

<https://www.iaria.org/conferences2020/ICDS20.html>

November 21 - 25, 2020 - Valencia, Spain

Open Data and Privacy

Public organizations, as well as private enterprises, collect data directly as the input necessary for provisioning their services (like contact information about individuals and citizens) or indirectly as the byproduct of their service provisioning (like the process information related to the chain of actions and interventions). Governments want to proactively share their data sets with the public. Via this so-called Open Data approach, governments intend to improve their transparency, accountability and efficiency, to support participatory governance by citizens, to foster innovations and economic growth, and to empower citizens and businesses for making informed decisions. In order to achieve these objectives, public organizations strive to open their data sets as raw as possible. But the collected data often pertain to natural persons (e.g., citizens, clients, employees or partners) and therefore contain privacy sensitive personal information.

Opening such data as raw as possible is, therefore, subject to privacy risks (i.e., personal data disclosure risks) with adverse impacts on the fundamental human rights of individuals as well as on their dignity, liberty,

autonomy and income. Linking the opened data sets to other data sets can also reveal more privacy-sensitive information about individuals than that in those opened data sets. Consequently, protecting the privacy of citizens and individuals is an important precondition for governmental organizations for opening their data sets.

Big Data and Privacy

Further, we currently witness the rise of the Big Data paradigm as there are a huge amount of data being generated, collected, analyzed and distributed at a fast pace. This growth is due to the proliferation of many connected devices (such as cameras, smart phones, sensors, and smart household appliances), widespread and intensive usage of social networks, and digital transformation of business and organizational processes and services. There is a growing demand to make use of Big Data and develop (new) applications and services that ease our daily lives, create added values for businesses, provide insight in societal phenomena, and guide policymaking processes. Often Big Data usage does not fully coincide with the purpose for which the data were originally collected. Using the Big Data gathered from various sources and for diverse purposes, for example, can violate privacy rights of individuals and result in personal data disclosures. On the one hand, the data growth makes it difficult to detect and deal with those data disclosure risks that are hidden in the data set (i.e., the intrinsic risk factors). On the other hand, the growth of other data sets (i.e., the increase of the so-called background knowledge available to other parties) makes it difficult to assess and deal with the data disclosure risks that may arise when combining own data sets with the other data sets (i.e., the extrinsic risk factors). Consequently, Big Data makes it difficult for data controllers to share their data with specific groups, individuals or the public in responsible way.

Topics suitable for the special track:

The aim of this track is to foster research on methodologies, concepts, policies, procedures and technologies that contribute to protecting personal information in Open Data and/or Big Data settings, while preserving their utility for addressing societal issues and creating added business values. We invite the researchers and practitioners from academia, industries and public organizations to present their innovative (applied) research results or novel approaches and methods related, but not limited, to the following topics:

- Applications areas of Big & Open Data in a responsible way like: policymaking, healthcare, e-learning, economics, insurance, and business.
- Data protection technologies, procedures and policies in Big & Open Data settings like: data protection governance, economics of privacy, privacy enhancing architectures, frameworks, mechanisms and tools, design aspects of socio-technological systems (e.g., the privacy by design and default aspects), data minimization technologies (e.g., statistical disclosure control methods and tools), legal aspects of data protection (in light of, e.g., the GDPR), artificial intelligence and privacy, and pilots and use cases.
- Other relevant topics include data quality issues, misinterpretation and misunderstanding aspects, and ethical issues (e.g., discrimination). Note that the submitted work should be related to the general topic of the track in some way. In case of any doubt please feel free to contact the track chairs.

Contribution Types

- Regular papers [in the proceedings, digital library]
- Short papers (work in progress) [in the proceedings, digital library]
- Posters: two pages [in the proceedings, digital library]
- Posters: slide only [slide-deck posted on www.iaaria.org]
- Presentations: slide only [slide-deck posted on www.iaaria.org]
- Demos: two pages [posted on www.iaaria.org]

Important Datelines

- Inform the Chair: As soon as you decide to contribute

Submission: September 21

Notification: October 11

Registration: October 21

Camera-ready: October 21

Note: The submission deadline is somewhat flexible, providing arrangements are made ahead of time with the chair.

Paper Format

- See: <http://www.aria.org/format.html>

- Before submission, please check and comply with the editorial rules: <http://www.aria.org/editorialrules.html>

Publications

- Extended versions of selected papers will be published in IARIA Journals: <http://www.ariajournals.org>

- Print proceedings will be available via Curran Associates, Inc.: <http://www.proceedings.com/9769.html>

- Articles will be archived in the free access ThinkMind Digital Library: <http://www.thinkmind.org>

Paper Submission

<https://www.ariasubmit.org/conferences/submit/newcontribution.php?event=ICDS+2020+Special>

Please select Track Preference as **PPODS**

Registration

- Each accepted paper needs at least one full registration, before the camera-ready manuscript can be included in the proceedings.

- Registration fees are available at <http://www.aria.org/registration.html>

Contact

Chairs:

Sunil Choenni: sunilchoenni@gmail.com

Mortaza S. Bargh: mortaza.bargh@gmail.com

Logistics: steve@aria.org