Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

Research Seminar

Empowering the Data Subject in Anonymization: Verifiability, Transparency and Co-Utility

Josep Domingo-Ferrer
UNESCO Chair in Data Privacy, Universitat Rovira i Virgili, Catalonia

10-11am Monday 15Th June 2015

Abstract: There are currently two approaches to anonymization: "utility first" (use an anonymization method with suitable utility features, then empirically evaluate the disclosure risk and, if necessary, reduce the risk by possibly sacrificing some utility) or "privacy first" (enforce a target privacy level via a privacy model, e.g., k-anonymity or ε-differential privacy, without regard to utility). To get formal privacy guarantees, the second approach must be followed, but then data releases with no utility guarantees are obtained. Also, in general it is unclear how verifiable is anonymization by the data subject (how safely released is the record she has contributed?), what type of intruder is being considered (what does he know and want?) and how transparent is anonymization towards the data user (what is the user told about methods and parameters used?).

We show that, using a generally applicable reverse mapping transformation, any anonymization for microdata can be viewed as a permutation plus (perhaps) a small amount of noise; permutation is thus shown to be the essential principle underlying any anonymization of microdata, which allows giving simple utility and privacy metrics. From this permutation paradigm, a new privacy model naturally follows, which we call (d, v)-permuted privacy. The privacy ensured by this method can be verified by each subject contributing an original record (subject-verifiability) and also at the data set level by the data protector. We then proceed to define a maximum-knowledge intruder model, which we argue should be the one considered in anonymization. Furthermore, we make the case for anonymization transparent to the data user, that is, compliant with Kerckhoff's assumption (only the randomness used, if any, must stay secret). Finally, we discuss co-utility in collaborative anonymization of microdata by the data subjects themselves.

Venue: Large Conference Room, O'Reilly Institute.

Further Details: Doug Leith (doug.leith@tcd.ie)

Future Cities
Trinity Centre for Smart and Sustainable Cities

ADAPT
Engaging Content
Engaging People