Objective

Protecting user’s online behaviour is a challenging privacy problem. In this project, we will develop communication protocols for metadata privacy. Metadata is implicit information, such as when and how many messages are sent, and can therefore not be protected using standard encryption. Unlike encryption, metadata privacy is not currently available in instant messaging services, due to the impracticality of current protocols.

To protect users, developing new, practical protocols for metadata privacy is therefore essential. Moreover, metadata privacy is a EU priority, which will be regulated by the ePrivacy Regulation that is currently being drafted. Consequently protocols that guarantee metadata privacy for instant messaging needs to be designed to meet EU’s needs.
We propose a holistic project to address metadata privacy, ranging from conceptual design to implementations of protocols in software. By combining Nelson’s background in privacy, and Askarov’s expertise in formal methods, we expect to be able to tackle metadata privacy from a new perspective. Specifically, we will design protocols that are provably private. That is, we will guarantee that our protocols are free from unintentional leakages. In addition, our protocols will be designed to be feasible to use on battery constrained devices such as phones.

**Fields of science**

natural sciences > computer and information sciences > software

**Programme(s)**

HORIZON.1.2 - Marie Skłodowska-Curie Actions (MSCA)  [MAIN PROGRAMME]

**Topic(s)**

HORIZON-MSCA-2021-PF-01-01 - MSCA Postdoctoral Fellowships 2021

**Call for proposal**

HORIZON-MSCA-2021-PF-01

See other projects for this call

**Funding Scheme**

HORIZON-AG-UN - HORIZON Unit Grant

**Coordinator**

AARHUS UNIVERSITET

Net EU contribution

€ 214 934,40