Online identity and key new technologies
Rather than being closely related to specific technologies, devices or applications, questions of identity are here framed as a series of interactions in multiplex socio-technical systems. In an online context, identity as a theoretical construct is closely related to questions of data, privacy and rights (including, but not limited to digital rights). It thus becomes necessary to address and determine the relationships between data (all data/private data) and identity.

1. Current barriers & challenges identified by participants

1.1 Existing socio-technical barriers

- **Diverging definitions**

Identity is not easy to define, and current definitions are diverging. There is a need for the development of common definitions, and vocabularies enabling a multidisciplinary discussion of identity.

- **Society conceives identity as stable**

Identity (e.g. surname, passport, etc.) is predominantly conceived as being stable by society/policy-makers and in societal contexts. Yet, in scholarly discourses and research on identity, identity is often characterised as inherently dynamic. In addition, individuals might very well experience their identity/-ies as dynamic. This clash between the two opponent stances is currently not sufficiently addressed.

1.2 Current/future socio-technical challenges

- **Developing tools for managing online identity, including multi-scale filtering of content**

End-users could benefit from having a set of tools assisting the management of their online identities across platforms. As applications are increasingly bridged and interwoven, users need assistance in understanding the implications of this on the sharing of their data, and identity/-ies. Designing tools that enable multi-scale filtering of content by users, e.g. by giving more control of which date/information is accessible to whom, is a immediate challenge to be addressed.

- **Acknowledging and managing identifying features of large-scale data**

In an online/networked environment, users leave digital footprints behind. These footprints are data that can be harnessed or misused by third parties. In addition hereto, more sophisticated methods for analysing large-scale data from e.g. achieved system logs, mobile phone uses, and online actions by users, make is possible to identify individuals based on their preferences, patterns and social networks. This places an increased onus on developers, legislators, third parties and researchers to address and communicate the degree to which data reveal identity. Moreover, it poses the challenge of finding ways to anonymise individuals (data and identity).

- **Determining acceptable levels of anonymity online, and designing systems supporting these**

As current anonymity cannot really be granted online; single users can (with some effort) always be identified. It is important to determine which levels of anonymity should be allowed under which circumstances and contexts. Also, there is a need to address whether anonymity should form part of a more general set of digital rights. In extension of this, a challenge is to develop features that will allow for increasing levels of transparency for end-users. Individual users should be made aware of the level of, or lack of anonymity given systems allow for.

2. Moving forward: Strategies for bridging the gaps

- **Facilitating further formal and informal digital literacy education, which can equip users with more sophisticated tools for managing and understanding identity in online and hybrid contexts.**
- **Develop initiatives that raise awareness of issues related to identity-management in the 21st century.**
- **Fund interdisciplinary research that can an inform discussions on what constitutes identity, and how these can be translated into socio-technical system features.**