Threat Mechanism

Identifiability

Being able to sufficiently identify the subject within a set of subjects (i.e. the anonymity set)

Detectability

Being able to sufficiently distinguish whether an item of interest (IOI) exists or not. Detectability concerns IOIs of which the content is not known (to the attacker)

Unawareness

Being unaware of the consequences of sharing information

Non-compliance

Not being compliant with legislation, regulations, and corporate policies

Unanticipated revelation

Data reveals or exposes an individual or facets of an individual in unexpected ways. Unanticipated revelation arises from aggregation and analysis of large and/or diverse data sets

Linkability

Not being able to hide the link between two or more actions/identities/pieces of information

Non-repudiation

Not being able to deny a claim. The attacker can thus prove a user knows, has done or has said something

Disclosure of Information

The threat tree concerning information disclosure of data flow, data store, and process

Distortion

Inaccurate or misleadingly incomplete data is used or disseminated

Stigmatization

Data is linked to an actual identity in such a way as to create a stigma that can cause dignity losses or discrimination