Comments from Antonio Kung

|  |  |  |
| --- | --- | --- |
| Type | Comment | Suggested change |
| General | Report provide a definition of privacy engineering that does not conveys the need for an engineering process:  “collection of methods to support the mitigation of risks to individuals arising from the processing of their personal information within information systems”.  Report does say that it is not a definitive definition | Change the proposed definition to:  “collection of methods to support the engineering of systems that mitigate risks to individuals …” |
| Privacy risk management framework | Report explains the various process components of a privacy risk management framework.  It does not point out the need for an engineering process (this includes for instance the design of mitigation measures). | Reports should at least point out that the mitigation of risks should integrate an engineering process  It could refer to existing work (e.g. OASIS PMRM) |
| Privacy engineering objectives | Three privacy engineering objectives are defined (predictability, manageability, dissassociability)  These definitions are close to the protection goals defined by Marit Hansen, Meiko Jensen, Martin Rost (http://ieee-security.org/TC/SPW2015/IWPE/2.pdf):  Unlinkability, Transparency,  Intervenability. | A realignment of terms would be welcome.  The order is important. We would prefer the following order: dissassociability, predictability, manageability) |
| Privacy risk model | The section on privacy risk model defines impact (line 789) as follow: Impact is assessed as the magnitude of the problematic data action on the organization if occurs.  This is confusing because privacy breaches first have impact on citizens. | The distinction between the impact on the individuals and the organization must be made clearer.  For instance ligne 864 states that “the privacy risk model hinges on whether a data action becomes problematic for individuals”  As an example, if a private social network account content from one person is made public, the impact maybe huge for the person and negligible for the organization. |