From: Nigel Smart <nigel.smart@kuleuven.be>
Sent: Wednesday, October 23, 2019 10:32 AM
To: privacyframework <privacyframework@nist.gov>
Cc: Nigel Smart <nigel.smart@kuleuven.be>
Subject: NIST Privacy Comment

Hi Katie

Here are a couple of comments on the NIST Privacy Framework

Page 8: Line 271/272 I would rephrase as...

"For instance, if the organization is trying to achieve privacy by limiting observation, this may lead to implementing measures such as distributed data architectures or cryptographic privacy-enhancing technologies (PET) such as multi-party computation (MPC) or homomorphic encryption (HE_, or by using secure enclaves.
An organization may combine both PET and distributed data architectures and PETs.
The organization may also wish to achieve privacy by ensuring no data is trackable to specific individuals, for example by using statistical techniques such as differential privacy."

The above is clearer I think. It also uses the correct PET acronym that will enable readers to search the literature easier I think. Also there is no other mention in the doc for differential privacy, which seems a bit odd in a privacy document :-)

Page 27: Despite mentioning PET techniques on page 8 there is no mention in the PR.DS-P* things. To combine with PR.DS-P1 and PR.DS-P2 I would add the following ones...

PR.DS-PX: Where appropriate data-during-computation is protected using PETs technologies such as MPC/HE or secure enclave technologies.

PR.DS-PY: Where appropriate individual data records, and/or summary data, is protected using differential privacy techniques

Modify....

PR.DS-P1: Data-at-rest are protected via either appropriate encryption technolgies or distributed data architectures

Yours

Nigel

--
Nigel Smart
COSIC - KU Leuven