Privacy and Risk Task Force

Industry sector-agnostic

Overview

The Inputs and Semantics Working Group (ISWG) continues to define a data capture architecture consisting of immutable schema bases and interoperable overlays for Internet-scale deployment. The work being covered by the ISWG relates to all aspects of data harmonisation and data capture. This also includes the integration of all work being undertaken by the various Task Forces (TFs) and Focus Groups (FGs) housed under the ISWG, including the consent notice for purpose and jurisdictional privacy regulation work being undertaken by the Notice & Consent TF (NCTF). The assessment and risk analysis associated with data capture, data storage, data access and data sharing is not currently covered by any of the other TFs or FGs. The purpose of the Privacy & Risk Task Force (PRTF) is to bring recommendations on how OCA objects and other components can enhance necessary safety measures for privacy-friendly data usage.

Here is a quote to bring context to the proposed work of the PRTF from the recently published "Regulation of the European Parliament and of the Council on European data governance (Data Governance Act)":

"*There are techniques enabling privacy-friendly analyses on database that contain personal data, such as anonymisation, pseudonymisation, differential privacy, generalisation, or suppression and randomisation.*"

While OCA offers a global solution to semantic harmonization between data models and data representation formats, there is no strict control on defined attributes that could lead to correlation attacks on non-personal data which may become highly sensitive when aggregated.

The PRTF will analyse the requirements needed to formulate an expert overview on stricter Data Governance of private data with the objective of creating digital trust through transparency, human accountability and cryptographic assurance.

Mission and Scope

The mission of the *Privacy & Risk Task Force* (PRTF) is to create specifications, OCA objects and other components and best practices that fulfill the requirements for protecting privacy and to provide strong defensive technological enhancements to combat against subject re-identification when data is captured, stored and/or shared in an anonymized aggregated fashion.

With the exception of providing risk-based recommendations to other groups at ToIP, any governance decisions on privacy-related enhancements are out of scope for this task force. Governance questions will be done in close collaboration with Trust Assurance TF.

Intellectual Property Rights (Copyright, Patent, Source Code)

This TF uses the same IPR licensing selections as the Inputs and Semantics WG:

- Copyright mode: Creative Commons Attribution 4.0**.**
- Patent mode: W3C Mode (based on the W3C Patent Policy).
- Source code: Apache 2.0**.**

Conveners

- Jan Lindquist (Linaltec)
- Paul Knowles (Human Colossus Foundation)

Interested Members (add your name and organization if you may be interested in joining this TF)

- Paul Knowles (Human Colossus Foundation)
- Robert Mitwicki (Human Colossus Foundation)
- Jim St.Clair (Lumedic)
- Jay Fischbach (KABN)
- Scott Whitmire (Mayo Clinic)
- Scott Perry (scott Perry CPA)
- Ken Adler (ThoughtWorks)

Objectives

The objectives of the PRTF are to:

- Create specifications, white papers and other educational resources that provide enhanced insight on topics of innovation related to privacy and risk, including:
    - The development of tools to protect against re-identification, including any subsequent revisions to the Blinding Identity Taxonomy (BIT);
    - Defining re-identification risk types;
    - Implementing masking techniques for protecting privacy.
- Identification and analysis of any correlation risks encountered when combining data from different sources and the corresponding effects of those risks on privacy and data rights. This may include the introduction of a risk rating index as part of the ongoing work in this topic area.
- Introduction of any necessary controls to better enable:
    - Data masking and private data protection;
    - Synergy with the Notice and Consent Receipt work instigated by the Notice & Consent TF; and
    - Provision of recommendations for privacy and risk governance following enhanced risk reviews.
- Establish a ToIP liaison group for other standards bodies involved in risk management and risk assessment (ex. ISO 27000, ISO 31000, ISO 20899, GA4GH and Kantara)

Technical components

The privacy architecture will be built upon the core components of the Input and Semantics Working Group (ISWG). Any additional technologies and components that are deemed to be complementary to the overall mission, vision and scope of the DSWG by the majority of the members of the PRTF will be brought to the attention of the parent group for broader approval by the WG members.

Example use case

Deliverables

Proposed schedule

The scheduled time can be found here.

Meeting information

For meeting recordings refer to this link.

Meeting notes

Shared documents and links

Medical Information TF

https://wiki.trustoverip.org/display/HOME/Medical+Information+TF

Notice & Consent TF

https://wiki.trustoverip.org/pages/viewpage.action?pageId=66469

Regulation of the European Parliament and of the Council on European data governance (Data Governance Act)

https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-data-governance-data-governance-act

Aries RFC 0167: Data Consent Lifecycle

https://github.com/hyperledger/aries-rfcs/blob/master/concepts/0167-data-consent-lifecycle/README.md

Blinding Identity Taxonomy (BIT)

https://docs.kantarainitiative.org/Blinding-Identity-Taxonomy-Report-Version-1.0.pdf

ARX – Data Anonymization Tool

https://arx.deidentifier.org/

Aries RFC 0430: Machine-Readable Governance Frameworks

https://github.com/hyperledger/aries-rfcs/tree/master/concepts/0430-machine-readable-governance-frameworks