Open call - case studies of the use of privacy enhancing technology in multi-party collaborative analytics to tackle money laundering, fraud and other financial crime

Submissions of case studies should be sent to: aurora@bisih.org

A. Scope of invited case studies: technology

While 'privacy enhancing technologies' can be interpreted in a number of ways, this open call for submissions is focused on the following techniques.

Priority privacy enhancing techniques/technologies of interest (including blended technology solutions):

- differential privacy
- (partial/full) homomorphic encryption
- zero-knowledge proof
- secure multi-party computation
- trusted execution environments

However, financial crime and fraud investigation or prevention examples relevant to use-cases below using other techniques will also be considered.

B. Scope of invited case studies: use-cases

Case studies should ideally relate to anti-money laundering use-cases, both encompassing alert generation or investigation and 'know your customer' capabilities, and fraud prevention and identification. Other case studies where applicable technologies are used to combat other types of financial crimes or applied in highly regulated domains will also be considered.

Case studies are welcome from any jurisdiction or geographic region, including both national-level collaboration as well as cross-border collaboration initiatives. Use-cases that support privacy preserving analytical collaboration 'intra-group', i.e. across a multi-national financial institution, are also in scope.

Priority capabilities within the use-cases include:

- **Record linking.** Verification/matching of data attributes held by requesting parties against external reference data, without disclosure of the query or disclosure of the reference data.
- **Network mapping.** Network mapping of connected nodes (e.g. through transactions) across multiple data owners, without data owners' disclosure of underlying data.

- **Prevalence queries.** Macro-insights about the prevalence of certain rule-based queries across a community of data owners, without disclosure of underlying data or an individual data owner's prevalence exposure.
- **Regression analysis.** Analysis about the relationship between common data attributes across a community of data owners, without disclosure of underlying data.
- **Federated machine learning.** Analysing patterns across multiple data holdings without any disclosure of underlying data.

C. Scope of invited case studies: Technical readiness

A key element of the call for applications is to identify use of the privacy enhancing technologies in 'real-world' deployment on operational data relevant to anti-money laundering or fraud prevention and multi-party collaboration. Case study submissions should relate to deployment on 'real' personal data and in operational use, rather than initiatives only explored on synthetic data.

D. Use of information:

BISIH intends to use received case study material in a publicly available reference, report or research paper. Case study information submitted must not be confidential. BISIH will seek confirmation of approval from case study authors for BISIH material that features the case study before publication.

E. Type of entity invited to make a case study submission:

Case studies can be submitted from any relevant project owner with the authority to share the work and results of the PET project in question. This may include:

- A financial/payment service provider or groups such entities, making use of PET technology
- Commercial PET technology firms
- Academic PET initiatives
- A public sector agency benefiting from PET technology to support multi-party collaboration relevant to the threats

F. Value and impact of the work:

Case study submissions will be analysed and assessed for potential inclusion in a BISIH research publication.We intend that this work, and associated events, contributes to achieving the following goals:

- Supporting education and awareness-raising about PETs and the relevance to financial crime and fraud identification and prevention use cases, with specific relevance to financial information sharing partnerships;

- Encouraging greater clarity about the data protection implications of adoption of PETs for such use cases;
- Providing insight about specific opportunities, challenges and limitations to leverage PETs to enhance the effectiveness of anti-money laundering and fraud prevention outcomes through information-sharing; and
- Promoting international policy and regulatory dialogue about how to achieve an effective, secure and ethical environment for the growth of PET technology within financial information-sharing partnerships.

This BISIH project, supported by the case studies, will contribute to helping policy-makers and senior decision-makers in the private sector understand the state-of-the-art in technical deployment of PET techniques associated to financial crime and fraud prevention use-cases.

BISIH intends to develop an ongoing research relationship with entities that submit case studies and case study projects may be invited to participate in relevant research or profile-raising events, as well as being included in the research itself.

Annex A – case study submission form

Submissions of case studies should be sent to: aurora@bisih.org

Case study submission

Case study survey question	Response
1. **What is the name of the case study?** (This can be the branded name of the solution or a descriptive title for the case study)	
2. **What is the name of the PET technology company/companies involved in the case study project?**	
3. **What time period was the case study project active?** (Year of project commencement to year of project completion)	
4. **How many institutional participants were involved in the project and across which sectors?** (Name of companies where disclosable and, otherwise, the number of entities involved and their commercial sectors)	
5. **What was the information-sharing problem statement or objective for the project to address?**	
6. **Please describe the information information-flow process within this use-case, including…**	

	6.a) Describing the data attributes queried;	
	6.b) Describing the information query process (incl. the role of the requesting parties and the requested data owners);	
	6.c) Describing the information that is revealed (to whom); and	
	6.d) Describing the information within the process that remains undisclosed (by virtue of use of PETs).	
7. What PET techniques were used in this project? (Homomorphic encryption, multi-party secure computation, etc).		
8. Please describe the volume of data involved in the project.		
9. Please describe the timeliness of the exchange within this project? (Is it real-time, and – if not – what is the refresh frequency of data updates?)		
10. Please describe the readiness status of this case-study (technical readiness measures or reference to whether the case study represents a demonstration, pilot, or commercial deployment etc)		

11. What data quality and interoperability issues were identified between participating institutions and how were they resolved?	
12. What did the project achieve? (Please include any performance metrics that you have developed for the case study)	
13. What geography/legal jurisdiction(s) are relevant to the case study	
14. Any further comments relevant to the case study or lessons arising from the project to date?	

Case study submissions by:

Name	
Role	
Company	
Email	
Information correct as of what date:	