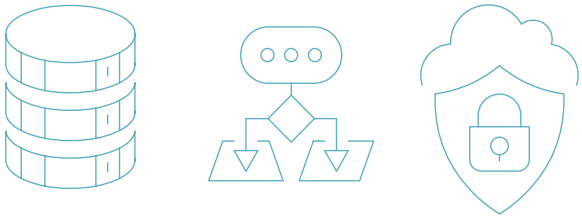
FATF



STOCKTAKE ON DATA POOLING, COLLABORATIVE ANALYTICS AND DATA PROTECTION

Technology has the potential to make efforts to combat money laundering and terrorist financing faster, cheaper, and more efficient.

This includes technology to facilitate data sharing and collaborative analysis, and help financial institutions analyse large amounts of data more efficiently and identify patterns and trends more effectively. Pooling data and using collaborative analytics can improve understanding, assessment, and mitigation of money laundering and terrorist financing risks. It can also help prevent criminals from exploiting information gaps, as they engage with multiple domestic and international FIs, each having a limited and partial view of transactions

New and emerging privacy-enhancing technologies offer promising ways for private sector collaboration while protecting information in specific use cases and in line with national and international data protection and privacy (DPP) frameworks. Privacy-enhancing technologies rely on a range of different cryptographic tools to enable privacy in various applications. These tools allow multiple parties to interact meaningfully to achieve an application goal, without revealing underlying private information to one another or to third parties.

Under its German Presidency, the FATF made it a priority to take stock of new technologies, and to identify when or how they could be used to improve AML/CFT efforts. By engaging with AML/CFT national authorities, financial institutions, technology developers, academia and other private sector representatives, this project examines commercially available and emerging technologies that can help financial institutions collaborate and carry out advanced AML/CFT analytics, in line with national and international data privacy and protection legal frameworks. The report also identifies the challenges that could prevent successful deployment of these innovative technologies and possible solutions and policy responses.

The report acknowledges that AML/CFT and data privacy and protection are both significant public interests that serve important objectives, which are neither in opposition nor inherently mutually exclusive.

WHY SHARE DATA?

Data sharing is critical to fight money laundering and the financing of terrorism and proliferation. Multinational criminal schemes do not respect national boundaries, nor do criminals or terrorists only exploit one institution to launder their ill-gotten gains or move or use funds with links to terrorism.

Customers are increasingly using multiple institutions for banking, instead of banking with a single financial institution with a large market share. This means that data about individual customers is becoming increasingly dispersed across a wide array of financial institutions. If multiple financial institutions share data and apply advanced analytics, it can reveal trends or potentially suspicious activities that could otherwise go undetected by a sole institution. This creates a further incentive for private-to-private data sharing and collaboration to bring together sufficient data sets to apply advanced analytics to more accurately assess customer risks or identify potential suspicious activity.

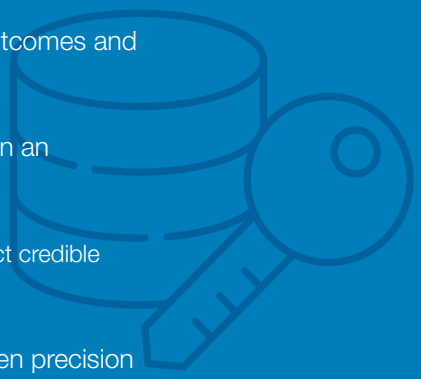
A primary reason to share or pool data is to **monitor transactions.** Sharing data could also facilitate **customer due diligence measure**s, such as institutional risk assessment, on-boarding customers, risk management of a business relationship, and identification of the beneficial owner. It can help **identify and share patterns and flows**, such as the identification of typologies of crime and intelligence-driven investigations.

An open dialogue between financial institutions AML/CFT supervisors and DPP authorities is important to the success of initiatives using new technologies and their ultimate effective implementation. In addition, regulatory sandboxes (or innovation hubs) provide valuable opportunities to test how new technologies interact with national (or supranational) AML/CFT and DPP laws and regulations.

WHICH TYPES OF TECHNOLOGIES CURRENTLY EXIST?

and how can they improve efforts to tackle money laundering and terrorist financing?

CRYPTOGRAPHY/ENCRYPTION TECHNOLOGIES



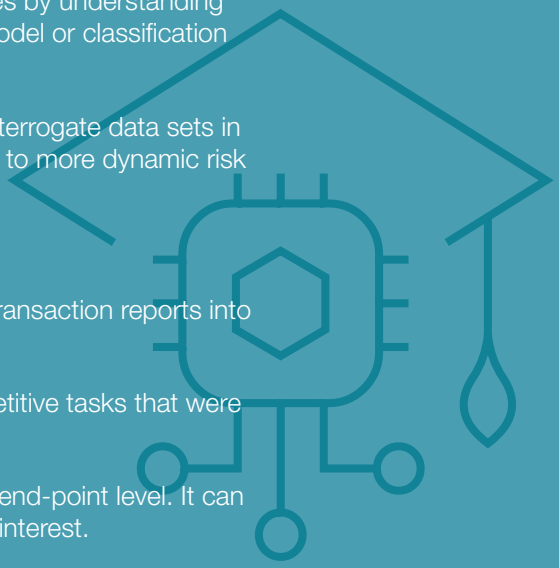
Homomorphic encryption enables access to a wider set of data to improve outcomes and enable intelligence-led decision making.

Zero-knowledge proofs allows one bank to establish another bank held data on an individual, without sharing that individual's identity.

Secure-multiparty computation when applied to disparate data sources, can extract credible suspicions from different parties, while keeping the data sovereign.

Differential Privacy can analyse broad trends, but may create a trade-off between precision of data and privacy.

ADVANCED ANALYTICS



Machine Learning can optimise decision points in business processes by understanding the current states and predicting optimal decisions. A scoring model or classification mode can help identify suspicious networks or entities.

Federated Learning such as a travelling algorithm, can access and interrogate data sets in different financial institutions without moving the data. This leads to more dynamic risk assessment tools.

Deep Learning can help financial institutions monitor transactions.

Natural language processing can transform free text in suspicious transaction reports into structured data that can be used for network analytics.

Robotic process automation enhances efficiency by automating repetitive tasks that were previously performed by humans.

Network Analytics derives patterns that cannot otherwise be seen at end-point level. It can identify network of related entities based on known subject(s) of interest.

INFRASTRUCTURES FOR PROCESSING AND TRANSFER

Trusted execution environments (confidential computing) | for example, two parties agree to share their data (e.g., transaction data) and analyse it using a trusted execution environment.

Secure cloud technology | enable firms to collect, store, and analyse significantly large data sets at very low costs, of both structured and unstructured data, that can help collaboration amongst those with access to the secure cloud environment. However, legal barriers for data sharing remain the same.

Distributed Ledger Technology | can be used to share data between several parties, without one party having the full power of data disposal.

WHAT ARE THE **CHALLENGES** AND **POSSIBLE POLICY RESPONSES** TO USING NEW TECHNOLOGIES FOR DATA SHARING AND COLLABORATIVE ANALYSIS?

Data privacy and protection requirements represent a key policy consideration. This is due to the perceived conflict between a financial institution's desire to share information and more efficiently comply with AML/CFT measures, and existing legal restrictions designed to protect the privacy of its customers. However, as outlined in the report, new technologies that involve the encryption of sensitive personal data may offer innovative solutions to respect diverging national and international DPP laws and allow for the exchange and analysis of information for AML/CFT purposes.

Data quality and data standardisation are important elements to the overall accuracy of collaborative analytics. Low quality data, including inaccurate or out-of-date data, could also nullify the benefits of data pooling and collaborative analytics. It could result in an erroneous analytical outcome, including biased conclusions, and in a worst case scenario, contribute to financial exclusion.

Regulatory clarity in the form of explicit regulatory requirements and guidance for the use of new technology is often lacking. Without guidance and certainty from regulators, there is less incentive to invest and implement new technological solutions for collaborative analytics.

Explainability and interpretability of a decision based on a high level of automation is crucial. Regulators could work with public and private sector technologists and other relevant stakeholders to evaluate and help drive adoption of appropriate practices to explain, document, and govern advanced analytics in the context of AML/CFT. There also needs to be the possibility to manually intervene to review the outcome of advanced analytics (e.g., artificial intelligence and machine learning) to ensure the accuracy of the results and to continuously refine algorithmic models.

HOW CAN WE ENABLE THE **WIDER USE** OF **DATA POOLING** AND **ADVANCED ANALYTICS**?

PROMOTE REGULATORY CERTAINTY AROUND THE USE OF THESE NEW TECHNOLOGIES

Clear guidance from national financial regulators on the kinds of data that could be shared between FIs, and on whether certain technologies (e.g., homomorphic encryption, etc.) and processes enable organisations to remain compliant with national and supranational privacy requirements, in addition to the financial-sector-specific regulations. These assurances may encourage investments in technology, training, human resources, and production deployments of data sharing solutions.

PROMOTE ENABLING ENVIRONMENTS

Pilot programs, regulatory sandboxes and innovation hubs allow stakeholders to test new technologies for data sharing and analysis, without punitive or overly aggressive regulatory enforcement. Engagement with and involvement of national DPP authorities is essential to the success of such initiatives. Such engagement will ensure that technology is developed in alignment with AML/CFT and DPP requirements. It will promote common learning, and increased clarity on issues such as model governance, modelling techniques and how data analytics can target particular ML/TF risk areas and facilitate data sharing, while respecting individuals' right to data protection and privacy.

BIAS PREVENTION IN ARTIFICIAL INTELLIGENCE

Advanced analytics using artificial intelligence systems should be designed in a way that respects the rule of law, human rights, democratic values and diversity. Therefore, it is important to regularly review the legitimacy and credibility of data sources, extensive model validation, and continuous model monitoring to prevent human bias and discrimination in artificial intelligence.

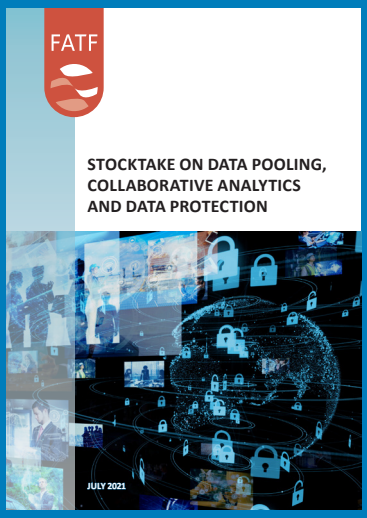
DATA STANDARDISATION AND GOVERNANCE

In order to enhance data quality, some respondents called for the standardisation of formats for data collection, data governance policies and controls, as well as to promote the use of open APIs to enable customers to share data between FIs.

WHAT IS **NEXT?**

The FATF will build upon this Stocktake report by continuing the dialogue between AML/CFT supervisors, technology developers, financial institutions, and DPP authorities, and other relevant experts.

This will ensure that new technologies that can contribute to enhanced AML/CFT effectiveness may be fully utilised, consistent with DPP national and international frameworks.

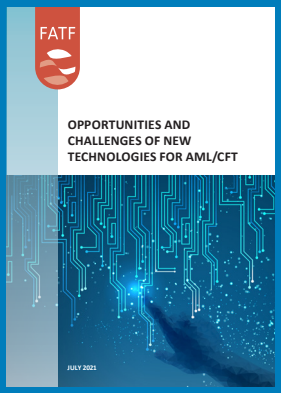


Download the complete report

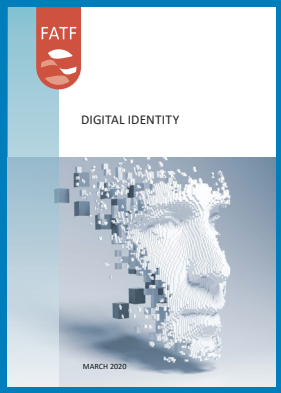
Stocktake on Data Pooling, Collaborative Analytics and Data Protection, 69 pages

From www.fatf-gafi.org

Also available on www.fatf-gafi.org :



Opportunities and Challenges of New Technologies for AML/CFT, July 2021



Digital Identity, FATF Guidance, February 2020