By: Lyons Liu, Dash Nunes, Brett Youngman

Privacy technologies for financial intelligence  A Data Bytes Company Project

Privacy Enhancing Technologies Use Case Scenario Discussion

Contents

[SUSPICIOUS PERSON LIST COMPARISON by Brett Youngman 2](#_Toc512763239)

[Overview 3](#_Toc2019168154)

[Use cases 3](#_Toc1239340210)

[Public to private 3](#_Toc147852420)

[Public to public – domestic trusted group 4](#_Toc1373422436)

[Public to public – international trusted group 4](#_Toc1578923753)

[Public to public – international untrusted group 4](#_Toc1685863986)

[Private to private – domestic trusted group 5](#_Toc1185864098)

[Private via public to private – domestic untrusted group 5](#_Toc746968940)

[SUSPICIOUS TRANSACTION DISCOVERY - MODEL COMPARISON AND SHARING 6](#_Toc1229742586)

[Use cases 6](#_Toc1831512530)

[SUSPICIOUS TRANSACTION DISCOVERY - DATASET SHARING 7](#_Toc573593424)

[Hypothetical use cases for Implementing PET by Dash Nunes 7](#_Toc1696411372)

[Use Case 1: Data Sharing Between Law Enforcement Agencies 8](#_Toc402446569)

[A real-world Hypothetical scenario: 8](#_Toc1608224978)

[The Case of the Stolen Diamonds: 9](#_Toc1909375632)

[Use Case 2: Information Sharing Between Banks and Financial Institutions 9](#_Toc1655960290)

[The Case of the Global Money Laundering Ring: 10](#_Toc1814863048)

[Use Case 3: Collaboration Between Public and Private Sector Entities 11](#_Toc2140412200)

[Uniting Against Financial Crimes: A Public-Private Partnership 11](#_Toc706235900)

[Use Case 4: Data Sharing Across International Borders 12](#_Toc1102447048)

[A Global Alliance Against Cybercrime: Bridging Borders with Privacy 13](#_Toc243929471)

[Use Case 5: Investigating Cybercrime 14](#_Toc2092560)

[What are the key blockers to a successful investigation? 14](#_Toc25175988)

[What is required for the investigation to be a success? 14](#_Toc1240250542)

[What are some potential privacy concerns in this scenario? 14](#_Toc1885183128)

[How can the three techniques assist with minimizing any privacy concerns in the aforementioned scenario? 14](#_Toc1150785207)

[What are some other techniques that can be used to assist with collaboration between multiple parties to prevent cybercrime? 14](#_Toc1979830289)

[Investigating a Cyberattack on an Australian Financial Institution 14](#_Toc1311367690)

[Financial Crime Investigations by Lyons Liu 15](#_Toc347771371)

[Overview: 16](#_Toc1799689241)

[Money Laundering Investigations: 16](#_Toc1365166114)

[Scenarios: 16](#_Toc295772690)

[Blockers 16](#_Toc1696505807)

[Privacy concerns 16](#_Toc1084063840)

[Techniques for privacy concerns 17](#_Toc1106380436)

[Techniques for collaboration 17](#_Toc2135202702)

[Cybersecurity Threat Detection: 17](#_Toc552113833)

[Scenarios: 17](#_Toc326712170)

[Blockers 18](#_Toc997957992)

[Privacy concerns 18](#_Toc1752635999)

[Techniques for privacy concerns 18](#_Toc1389515961)

[Insider Trading Investigation: 18](#_Toc1359316215)

[Scenarios: 19](#_Toc748692959)

[Blockers 19](#_Toc1303803096)

[Privacy concerns 19](#_Toc264035555)

[Techniques for privacy concerns 19](#_Toc59784275)

[Techniques for collaboration 19](#_Toc274573444)

[Cross-Border Payment Fraud: 20](#_Toc302273787)

[Scenarios: 20](#_Toc587633100)

[Blockers 20](#_Toc1419656870)

[Privacy concerns 20](#_Toc132678418)

[Techniques for privacy concerns 20](#_Toc1961402658)

[Supply Chain Financing Fraud: 21](#_Toc2086923340)

[Scenarios: 21](#_Toc711592352)

[Blockers 21](#_Toc177494737)

[Privacy concerns 21](#_Toc1677267994)

[Techniques for privacy concerns 22](#_Toc685689024)

[Techniques for collaboration 22](#_Toc316751885)

[Terrorist Financing Investigation: 22](#_Toc996408068)

[Scenarios: 22](#_Toc326804886)

[Blockers 23](#_Toc703939189)

[Privacy concerns 23](#_Toc904744490)

[Techniques for privacy concerns 23](#_Toc516308791)

[Techniques for collaboration 23](#_Toc1669200113)

[Identity Theft Ring: 24](#_Toc9119352)

[Scenarios: 24](#_Toc750073894)

[Blockers 24](#_Toc1227404825)

[Privacy concerns 24](#_Toc557479124)

[Techniques for privacy concerns 25](#_Toc736539208)

[Techniques for collaboration 25](#_Toc1408070554)

[Conclusion 25](#_Toc227845549)

[References: 26](#_Toc1898996980)

# SUSPICIOUS PERSON LIST COMPARISON by Brett Youngman

## Overview

Suspicious persons lists are collated periodically using one or many unique identifiers such as driver licence, passport or national ID number. All available identifiers (multiple passport numbers and licences per person) are compared against identity lists held by each participating party.

**Privacy considerations**

* **High trust situations** use existing security and governance arrangements to compare data and perform unencrypted operations on secure systems. Data is encrypted during transit and at rest.
* **Medium trust situations** require privacy preserving technology to compare data while encrypted. Governance arrangements must be developed between parties.
* **Low trust situations** require privacy preserving technology to compare data while encrypted. Governance arrangements must prevent data sharing unless a trusted party approves.

## Use cases

### Public to private

|  |  |  |
| --- | --- | --- |
| **Low trust** | **Encryption in transit, operation, rest** | **Results available to public only** |

Compare publicly held suspicious person lists (SPL) to the customer lists of private companies. SPL is push only – the public party pushes to the private parties for matching or the private parties push to the public party. Comparison results are available to the public party only. Private parties should remain unaware of results. Public parties can use the results to request additional information from private parties.

**Privacy**

This use case enables low trust comparison by maintaining data encryption during transit, operation and rest. It maintains privacy by ensuring the results are available to public parties only.

**Technology**

1. Homomorphic encryption (comparison)
2. Symmetric encryption (sharing results).

Binary result is returned for a request. The partner who is doing the request will decide on weather to disclose information on that person. You can use any identifier that is current or past to ID someone. The entity that is doing the matching will give all the identifiers they have available to the entity they would like to match. If there are additional identifiers, they you can make additional match requests iteratively.

Suggestion 1: identifying individuals. There is a technique called Probabilistic Signature (p-sig). Technique that can be used in the Australian scenario when there is no unique identifier. If the identifier is only available to one agency such as Austrac. They would not necessarily have that identifier. There can be access issues.

Suggestion 2: Investigate MPC (secure multiparty computation) this matches one scenario in MPC. Helps match who on your list is in a particular data base. It can be done efficiently.  Both parties will be able to know who the customers are who are the intersection between these two sects.

### Public to public – domestic trusted group

|  |  |  |
| --- | --- | --- |
| **High trust** | **Encryption in transit and at rest** | **Results available to all parties** |

Compare SPL to other SPL held by trusted domestic public parties. SPL is push only – a public party pushes the SPL to one or more domestic public parties for comparison. Results are available to all parties.

**Privacy**

This use case enables high trust comparison by maintaining data encryption during transit and rest, combined with trusted domestic public party security and governance arrangements. It maintains privacy by ensuring the results are available to trusted domestic public parties only.

**Technology**

1. Symmetric encryption (sharing full details)

### Public to public – international trusted group

|  |  |  |
| --- | --- | --- |
| **Medium trust** | **Encryption in transit, operation, rest** | **Results summary available to all parties** |

Compare SPL to other SPL held by trusted international public parties.  SPL is push only – a public party pushes the SPL to one or more international public parties for comparison. Results are available in summary only, with full details available on application to the public party holding the information.

**Privacy**

This use case enables medium trust comparison by maintaining data encryption during transit, operation and at rest, combined with trusted international security and governance arrangements. It maintains privacy by ensuring results are only available in summary to trusted international parties and requiring the consent of a data holder before full details are made available.

**Technology**

1. Homomorphic encryption (comparison)
2. Symmetric encryption (sharing summary and full details)

Possible use case for SMC.

### Public to public – international untrusted group

|  |  |  |
| --- | --- | --- |
| **Low trust** | **Encryption in transit, operation, rest** | **Results available to data holder only** |

Compare SPL to other SPL held by untrusted international public parties.  SPL is push only – a public party pushes the SPL to one or more international public parties for comparison. Results are only available to the data holder. The data holder must choose whether to share the results with the requesting public party and whether they share a summary or full details.

**Privacy**

This use case enables low trust comparison by maintaining data encryption during transit, operation and at rest. It maintains privacy by ensuring results are only available to the data holder which can choose whether to share results with the requesting public party.

**Technology**

1. Homomorphic encryption (comparison)
2. Symmetric encryption (sharing summary or full details)

Countries that you do not necessarily deal with often and have no trust in what they are going to do with your data. The first example of SMC or homomorphic encryption where only one or an intermediary will obtain the results. An international organisation like Interpol is a good example of this use case where it does not necessarily provide the results back to the party who requested the results.

### Private to private – domestic trusted group

|  |  |  |
| --- | --- | --- |
| **Medium trust** | **Encryption in transit, operation, rest** | **Results summary available to all parties** |

Compare SPL to other SPL held by trusted domestic private parties. Results available to all parties in summary, with full details available by mutual agreement.

**Privacy**

This use case enables medium trust comparison by maintaining data encryption during transit, operation, and at rest. It maintains privacy by ensuring only personal information related to suspicious *customers in common* is shared between private parties. Governance arrangements between the parties would need to be developed. Private parties likely could not rely on existing exceptions in privacy legislation related to law enforcement and would probably need to gain the consent of their customers through changes to company privacy policies and terms of service.

**Technology**

1. Homomorphic encryption (comparison)
2. Symmetric encryption (sharing summary or full details)

Can be problematic due to the law in most countries. Privacy legislation operates meaning that you need encryption throughout transit operation and at rest. Better suited for an international context rather than the Australian market. America potentially?

### Private via public to private – domestic untrusted group

|  |  |  |
| --- | --- | --- |
| **Low trust** | **Encryption in transit, operation, rest** | **Results summary available to public party** |

Compare SPL to other SPL held by untrusted domestic private parties. Results available to the public intermediary only, with summaries or full results made available to private parties at the discretion of the public party.

**Privacy**

This use case enables low trust comparison by maintaining data encryption during transit, operation, and at rest. It maintains privacy by ensuring only the public party receives personal information related to suspicious *customers in common.*

The public party may require changes to their enabling legislation to define their role as an intermediary between private parties, including changes or addition to prevent private parties from further disclosing personal information shared with them by the public party, not dissimilar to existing ‘tipping off’ provisions in Australia’s AML/CTF legislation.

**Technology**

1. Homomorphic encryption (comparison)
2. Symmetric encryption (sharing summary or full details)

Should be suited tot the Australian Environment, the results are only available to a public intermediary accessing as a broker who we want to match against all of these different people. Puts the private parties in contact under a governance arrangement.

## SUSPICIOUS TRANSACTION DISCOVERY - MODEL COMPARISON AND SHARING

**Process**

Models are developed by each party using their own data, then encrypted and shared in a federated learning process, undergoing multiple iterations to improve performance.

**Privacy considerations**

Not applicable.

### Use cases

**Public/private to public/private**

|  |  |  |
| --- | --- | --- |
| **Trust N/A** | **Encryption in transit** | **Results available to all parties** |

Share models and compare relative effectiveness to test and develop more effective models for detecting suspicious transactions. Results available to all parties.

**Privacy**

Models do not include personal information. Data is encrypted in transit for best practice and protection of commercial interests.

**Technology**

1. Federated learning (comparison and sharing)
2. symmetric encryption (protecting commercial interests).

Sharing private data that the models are based on. Sharing the models themselves that are available to the parties that are contributing. Anyone can try out the model and test the best model that suits the data. This can be a good approach for smaller institutions. Larger institutions have more specialised models which could be less suitable.

## SUSPICIOUS TRANSACTION DISCOVERY - DATASET SHARING

**Process**

Datasets are shared between parties to allow development of new suspicious transaction detection methods.

**Privacy considerations**

Individual personal information within the dataset must be protected. The dataset should meet privacy standards and successfully resist reconstruction attacks.

**Use cases**

**Public to public/private**

|  |  |  |
| --- | --- | --- |
| **Low trust** | **No encryption** | **Results available to all parties** |

Share transaction datasets to enable public and private parties to test suspicious transaction discovery models. Results available to all parties.

**Privacy**

Dataset must guarantee privacy mathematically using differential privacy or similarly effective techniques. Dataset must successfully resist reconstruction and other attacks designed to identify individual persons within the data. If the dataset is released in its entirety, it does not need to resist timing or floating-point attacks.

**Technology**

1. Differential privacy

Injecting noise into the data set to share the data set and works on plausible deniability so you cannot confirm if someone is in the data set. Making data generally available, generally sensitive data and not a common use case.

# Hypothetical use cases for Implementing PET by Dash Nunes

## Use Case 1: Data Sharing Between Law Enforcement Agencies

**Key Blockers:**

* Lack of standardized data formats and protocols can hinder data integration and analysis.
* Legal and regulatory barriers may restrict data sharing between jurisdictions.
* Technical challenges in ensuring secure and authorized data access.

**Success Criteria:**

* Establish clear legal frameworks and regulatory guidance for data sharing.
* Develop standardized data formats and protocols for seamless data integration.
* Implement secure data sharing platforms and protocols to protect sensitive information.

**Privacy Concerns:**

* Unauthorized access to sensitive personal and financial information.
* Misuse of shared data for purposes beyond the scope of the investigation.
* Potential for data breaches and identity theft.

**Techniques to Minimize Privacy Concerns:**

* Employ privacy-preserving analytics (PPA) techniques to analyze data without revealing the underlying data itself.
* Utilize secure multi-party computation (SMPC) to enable multiple parties to compute a function on their data without revealing their individual data to each other.
* Implement homomorphic encryption to allow for computations to be performed on encrypted data without decrypting it first.

**Additional Collaboration Techniques:**

* Establish joint investigation teams (JITs) with clear roles and responsibilities.
* Utilize secure communication channels and protocols for timely and efficient information exchange.
* Foster a culture of trust and cooperation among participating parties.

**A real-world Hypothetical scenario:**

**The Case of the Stolen Diamonds:**

A renowned jewelry store in the heart of Sydney, NSW had been robbed of a collection of priceless diamonds. Detectives from the NSW Police were baffled, with no clear leads or suspects. The stolen diamonds had vanished without a trace, leaving behind a trail of unanswered questions.

Unwilling to give up, the NSW Police sought assistance from The Australian Federal Police (AFP), hoping to combine their resources and expertise to crack the case. The AFP agreed to collaborate, but the challenge remained: how could two agencies with different data formats, legal restrictions, and security protocols work together effectively?

The answer lay in privacy-preserving analytics (PPA), a set of techniques that allow for data analysis without revealing the underlying data itself. With PPA, the NSW Police and AFP could share relevant information without compromising the privacy of individuals or violating data sharing regulations.

Using secure multi-party computation (SMPC), the two agencies could combine their data and perform joint analyses without revealing their individual datasets. This allowed them to identify patterns and connections that might have been missed if they had worked in silos.

Further, homomorphic encryption enabled them to perform computations on encrypted data, ensuring that sensitive information remained protected throughout the investigation. This allowed them to analyse financial transactions, communication records, and other sensitive data without exposing it to unauthorized parties.

As the investigation progressed, the NSW Police and AFP established a joint investigation team (JIT) with clear roles and responsibilities. They utilized secure communication channels and protocols to exchange information swiftly and efficiently, fostering a culture of trust and cooperation.

Through their collaboration and the use of PPA techniques, the NSW Police and AFP uncovered a network of international smugglers involved in the diamond heist. They were able to track down the stolen gems and apprehend the perpetrators, bringing justice to the victims and restoring faith in law enforcement's ability to collaborate across jurisdictions.

This hypothetical story highlights the potential of privacy-preserving analytics in enabling law enforcement agencies to overcome barriers and work together effectively to solve complex crimes. By leveraging PPA techniques, agencies can share valuable information, identify patterns, and bring criminals to justice while protecting the privacy of individuals.

## Use Case 2: Information Sharing Between Banks and Financial Institutions

**Key Blockers:**

* Competitive concerns and reluctance to share sensitive information.
* Incompatible data formats and systems can hinder data integration.
* Lack of standardized protocols for secure data sharing.

**Success Criteria:**

* Develop industry-wide standards for data formats and sharing protocols.
* Establish secure platforms for sharing information while protecting confidentiality.
* Implement clear guidelines and procedures for data sharing and collaboration.

**Privacy Concerns:**

* Unauthorized access to customer financial data and transaction history.
* Misuse of shared information for profiling or targeted marketing.
* Potential for data breaches and reputational damage.

**Techniques to Minimize Privacy Concerns:**

* Aggregate and anonymize data before sharing to reduce the risk of identifying individuals.
* Utilize data masking techniques to protect sensitive information while preserving utility.
* Implement robust access controls and monitoring mechanisms to prevent unauthorized data access.

**Additional Collaboration Techniques:**

* Establish industry-led initiatives to promote information sharing and collaboration.
* Utilize real-time information sharing protocols to identify and prevent suspicious activity.
* Engage in joint training and education programs to enhance expertise in financial crime prevention.

The Case of the Global Money Laundering Ring:

A sophisticated money laundering ring had been operating undetected for years, channeling illicit funds through a web of shell companies and offshore accounts. The ring's activities spanned multiple countries and financial institutions, making it difficult for any single entity to track and disrupt their operations.

Concerned about the escalating threat of financial crime, a group of leading banks and financial institutions decided to collaborate in an unprecedented initiative to combat money laundering. They recognized that their siloed approach to data sharing was hindering their ability to identify and stop these criminal networks.

To address this challenge, they adopted industry-wide standards for data formats and sharing protocols, enabling them to seamlessly exchange information without compromising compatibility. They also established secure platforms for sharing data, ensuring that sensitive customer information remained protected.

Utilizing privacy-preserving techniques, they could aggregate and anonymize data before sharing it, reducing the risk of identifying individuals while preserving the utility of the information. Data masking techniques were also employed to further safeguard sensitive details.

To minimize the risk of unauthorized data access, they implemented robust access controls and monitoring mechanisms, including multi-factor authentication and continuous data auditing. This layered approach ensured that only authorized personnel could access shared data and that any unauthorized attempts were promptly detected and thwarted.

Through their collaboration, the banks and financial institutions were able to identify suspicious transaction patterns and connections that had previously gone unnoticed. They could then share this information in real-time, enabling them to collectively disrupt the money laundering ring's operations.

## Use Case 3: Collaboration Between Public and Private Sector Entities

**Key Blockers:**

* Differences in legal frameworks and data protection requirements.
* Lack of trust and transparency between public and private entities.
* Technical challenges in integrating public and private sector data systems.

**Success Criteria:**

* Establish clear legal frameworks and memoranda of understanding (MOUs) governing data sharing.
* Implement secure platforms and protocols for interoperable data exchange.
* Foster open communication and collaboration between public and private sector stakeholders.

**Privacy Concerns:**

* Potential for unauthorized access to personal data by public sector entities.
* Misuse of shared data for surveillance or other purposes beyond the scope of the collaboration.
* Erosion of public trust in both public and private institutions.

**Techniques to Minimize Privacy Concerns:**

* Implement data minimization practices, sharing only the minimum necessary information.
* Utilize privacy-enhancing technologies to protect sensitive data while enabling analysis.
* Establish clear data governance frameworks and oversight mechanisms.

**Additional Collaboration Techniques:**

* Develop joint risk assessments and threat intelligence sharing mechanisms.
* Establish joint working groups and task forces to address specific financial crime challenges.
* Foster a culture of shared responsibility and accountability for financial crime prevention.

Uniting Against Financial Crimes: A Public-Private Partnership

In the bustling financial hub of Melbourne, a surge in sophisticated financial crimes had left law enforcement and financial institutions grappling for solutions. The perpetrators, exploiting the complexities of the modern financial system, were laundering money, defrauding investors, and evading detection.

Recognising the need for a united front against these elusive criminals, the city's leading banks, financial institutions, and law enforcement agencies formed an unprecedented partnership. Their goal: to leverage their collective expertise and data to combat financial crimes while safeguarding privacy.

To bridge the gap between their different legal frameworks and data protection requirements, they established clear legal frameworks and memoranda of understanding (MOUs) governing data sharing. These agreements outlined the purpose, scope, and limitations of data sharing, ensuring that sensitive information was protected and used only for the agreed-upon purposes.

To facilitate interoperable data exchange, they implemented secure platforms and protocols that enabled seamless communication and data transfer between public and private entities. These platforms incorporated robust encryption, access controls, and auditing mechanisms to prevent unauthorized access and ensure the integrity of shared data.

To foster open communication and collaboration, they established regular meetings, joint working groups, and task forces to address specific financial crime challenges. These forums provided a platform for sharing expertise, identifying trends, and developing coordinated strategies to combat emerging threats.

To address privacy concerns, they implemented data minimization practices, sharing only the minimum necessary information to achieve their objectives. They also utilized privacy-enhancing technologies, such as homomorphic encryption and anonymization techniques, to protect sensitive data while enabling analysis.

To ensure accountability and transparency, they established clear data governance frameworks and oversight mechanisms. These frameworks defined roles and responsibilities for data management, access, and usage, while oversight mechanisms provided regular audits and reviews to ensure compliance and prevent misuse.

## Use Case 4: Data Sharing Across International Borders

**Key Blockers:**

* Divergent data protection laws and regulatory frameworks across jurisdictions.
* Lack of harmonized standards for data sharing and interoperability.
* Geopolitical tensions and concerns about data sovereignty.

**Success Criteria:**

* Establish international treaties and agreements to facilitate cross-border data sharing.
* Implement standardized data formats and protocols for global interoperability.
* Develop mechanisms for dispute resolution and mutual legal assistance.

**Privacy Concerns:**

* Potential for unauthorized access to personal data by foreign authorities.
* Misuse of shared data for political or social control purposes.
* Erosion of public trust in data protection and cross-border data flows.

**Techniques to Minimize Privacy Concerns:**

* Employ anonymization and pseudonymization techniques to protect sensitive data.
* Implement strong data governance frameworks and oversight mechanisms.
* Foster transparency and accountability in cross-border data sharing practices.

**Additional Collaboration Techniques:**

* Establish international law enforcement cooperation mechanisms and joint investigation teams.
* Utilize secure communication channels and protocols for effective collaboration.

A Global Alliance Against Cybercrime: Bridging Borders with Privacy

In the interconnected world of finance, cybercrime had become a global menace, with criminals exploiting the borderless nature of the internet to commit sophisticated frauds and attacks. To combat these threats, international cooperation was essential, but data sharing across jurisdictions was hindered by divergent data protection laws, regulatory frameworks, and geopolitical sensitivities.

The United States, with its robust data protection framework, the General Data Protection Regulation (GDPR), and Australia, with its Privacy Act 1988, faced unique challenges in collaborating on cross-border data sharing. However, recognizing the urgency of the situation, both countries embarked on an unprecedented initiative to bridge the regulatory divide and facilitate the exchange of critical information to combat cybercrime.

To address the issue of divergent data protection laws, they initiated negotiations for an international treaty that would establish harmonized standards for data sharing and interoperability. The treaty would outline the purpose, scope, and limitations of data sharing, ensuring that sensitive information was protected and used only for agreed-upon purposes.

To facilitate global interoperability, they collaborated on developing standardized data formats and protocols that would enable seamless communication and data transfer between US and Australian law enforcement agencies. These protocols would incorporate robust encryption, access controls, and auditing mechanisms to prevent unauthorized access and ensure the integrity of shared data.

To address geopolitical tensions and concerns about data sovereignty, they established a framework for dispute resolution and mutual legal assistance. This framework would provide a mechanism for resolving any disputes arising from data sharing activities and ensure that both countries had access to necessary information to pursue criminal investigations.

To minimize privacy concerns, they employed anonymization and pseudonymization techniques to protect sensitive data. These techniques would remove or mask personal identifiers, such as names and addresses, while preserving the utility of the data for analysis and investigation.

To ensure accountability and transparency, they implemented strong data governance frameworks and oversight mechanisms. These frameworks would define roles and responsibilities for data management, access, and usage, while oversight mechanisms would provide regular audits and reviews to ensure compliance and prevent misuse.

Through this collaborative effort, the US and Australia were able to establish a secure and effective cross-border data sharing mechanism that enabled them to effectively combat cybercrime. Their shared risk assessments and threat intelligence sharing mechanisms allowed them to anticipate and respond to emerging threats, while their joint investigation teams facilitated the coordination of cross-border investigations.

As a result, the global cybercrime network faced a formidable alliance of law enforcement agencies, empowered by shared data and unwavering commitment to protecting the digital economy. This hypothetical story demonstrates the power of international cooperation and privacy-preserving techniques in safeguarding the global financial system and protecting the public from cybercrime.

## Use Case 5: Investigating Cybercrime

**Key areas of interest:**

What are the key blockers to a successful investigation?

* Difficulty in attributing cyberattacks to specific individuals or groups
* Complex and ever-evolving nature of cyber threats
* Cross-border nature of cybercrime

What is required for the investigation to be a success?

* Advanced cybersecurity tools and expertise
* Enhanced global cooperation in cybersecurity
* Clear legal frameworks for addressing cybercrime

What are some potential privacy concerns in this scenario?

* Intrusion into individuals' digital devices and networks
* Collection and analysis of vast amounts of personal data
* Potential for misuse of data for law enforcement or intelligence purposes

How can the three techniques assist with minimizing any privacy concerns in the aforementioned scenario?

* PPA can allow for analysis of cybersecurity data without revealing the underlying personal data or sensitive information.
* SMPC can allow multiple parties, such as law enforcement agencies, cybersecurity firms, and private companies, to collaborate on investigations without sharing their individual data with each other.
* Homomorphic encryption can allow for analysis of cybersecurity data without decrypting it first, preserving the confidentiality of the data while enabling effective investigations.

What are some other techniques that can be used to assist with collaboration between multiple parties to prevent cybercrime?

* Information-sharing platforms specifically designed for cybersecurity
* Joint investigations between law enforcement agencies and cybersecurity experts
* Public-private partnerships to address cybercrime challenges

Investigating a Cyberattack on an Australian Financial Institution

**Background:**

A sophisticated cyberattack has targeted a major Australian financial institution, compromising sensitive customer data and disrupting financial transactions. The attack has left the institution scrambling to contain the damage, restore services, and protect its reputation.

**Key Blockers to Successful Investigation:**

**Attribution:** Identifying the individuals or groups responsible for the attack poses a significant challenge. Cybercriminals often employ sophisticated techniques to mask their identities and cover their tracks, making it difficult to trace the attack back to its source.

**Complexity:** Cyber threats are constantly evolving, with new attack methods and vulnerabilities emerging regularly. This makes it difficult for law enforcement and cybersecurity experts to keep up with the latest threats and effectively investigate cyberattacks.

**Requirements for a Successful Investigation:**

**Advanced Cybersecurity Tools:** Law enforcement agencies and cybersecurity firms need access to advanced cybersecurity tools and expertise to effectively investigate cyberattacks. These tools can help identify and analyze attack vectors, collect evidence, and track the movement of stolen data.

**Global Cooperation:** Enhanced global cooperation in cybersecurity is essential to combat cybercrime effectively. Information sharing, joint investigations, and coordinated responses can significantly improve the chances of identifying and apprehending cybercriminals.

**Techniques to Minimize Privacy Concerns:**

**PPA:** Privacy-preserving analytics (PPA) can be used to analyze cybersecurity data without revealing the underlying personal data or sensitive information. This allows investigators to extract valuable insights while protecting individuals' privacy.

**SMPC:** Secure multi-party computation (SMPC) enables multiple parties, such as law enforcement agencies, cybersecurity firms, and private companies, to collaborate on investigations without sharing their individual data with each other. This facilitates collaborative investigations while protecting sensitive data.

**Homomorphic Encryption:** Homomorphic encryption allows for analysis of cybersecurity data without decrypting it first. This ensures that the confidentiality of the data is preserved while enabling investigators to perform necessary analysis.

# **Financial Crime Investigations by Lyons Liu**

## Overview:

Financial Crime is crime that acts performed by individual or group to gain financial or professional benefits by stealing or unlawful taking other’s money or properties.

Financial Crime investigations are always involved with multiple parties, which would be financial institutions, law enforcement agencies, technology provider, businesses, jurisdictions across multiple countries and etc.

There are few scenarios of financial crime investigation listed below.

## Money Laundering Investigations:

### Scenarios:

Money laundering is involved with process of placement, layering and integration illegal money from illicit activity to other legal money or financial assets. Generally, financial institutions detect suspected money laundering activities through Know-Your-Customer (“KYC”), customer due diligence and daily monitoring system, and submit suspicious activity report to relevant regulatory bodies, law enforcement agencies and government.

As part of investigation, financial institutions may share transaction records, customer information, and suspicious activity reports with multiple banks and jurisdictions across multiple countries, it’s required to coordinate with national law enforcement agencies, legal teams from different countries, technology providers and etc. to trace and investigate the money laundering network.

### Blockers

* Complexity of Financial transactions, which required advanced analytics and forensic accounting, and also how to exposure disguise by using latest techniques.
* It’s harder to crack the encryption or anonymize of the financial transactions.
* Diverse systems and protocols between financial institutions or other parties, which may be challenges to aggregating and analysing data.
* Data privacy laws and regulations.
* Cross board investigation may complex the investigation process and slower down the investigations.

### Privacy concerns

* Sensitive financial data of individual. It’s essential to ensure privacy and confidentiality of individual whose data has been shared, and investigation parties need to decide/agree clear scope, control of data sharing and data protection standard.
* Advanced techniques like artificial intelligence and machines learning for data analysis may increase concerns of impacts on individual privacy.
* Data retention period may lead to misuse or unexpected data leak.
* Disclosure of investigations may impact individuals’ privacy and reputation who are not convicted.
* Risk of data breaches compromising investigative information.

### Techniques for privacy concerns

* Anonymization and aggregation techniques to protect individuals' identities while still extracting meaningful insights from financial data.
* Role based data access restriction, example tokenization platforms.
* Encryption of personal and sensitive information during storage and transmission, example homomorphic encryption (computations on encrypted data without revealing the raw information) or encrypted communication platforms.
* Implement safeguards to prevent biases and misuse of AI & ML in investigations, example federated learning (machine learning model training across decentralized devices), adding noise to data without impacting accuracy.

### Techniques for collaboration

* Standardized encrypted and secure platform is used for secured and real time sharing.
* Cross board cooperation agreements.

Parties involved in investigation can set up centralized coordination centres.

* Standardized data formats and protocols are used for sharing investigation or highly confidential information.

## Cybersecurity Threat Detection:

### Scenarios:

Cyberattack is generally performed by individuals, targeted on banks, insurance companies, and other financial institutions for data stolen and operational or system damage. Financial institutions normally detect anomalies through daily monitoring activities of networks and operations, would also have work with regulatory bodies, cybersecurity firms, government, and other technology providers to safeguard its systems.

### Blockers

* Large number of false alerts makes it challenging to identify and prioritize genuine threats, potentially resulting in critical threats being overlooked.
* Complex IT environments with numerous interconnected systems and applications, especially for big companies with legacy systems and outdated technology.
* Encrypted communications can hide malicious activities, impeding threat detection.
* Sophistication of Cyber Attacks.

### Privacy concerns

* User profiling and behavioural Analysis may lead to unwarranted scrutiny and profiling of innocent individuals.
* Cybersecurity threat detection systems often require access to financial data to identify suspicious activities. However, the access to and analysis of personal financial information must be done with strict adherence to privacy regulations to prevent unauthorized disclosure.
* Extended retention periods increase the likelihood of unauthorized access, and individuals may be concerned about the long-term storage of their personal information.
* Ethical and Legal considerations is required, while performing detection activities.

### Techniques for privacy concerns

* Utilize anonymization and pseudonymization techniques.
* Encryption of required data and ensure secure transmission, example homomorphic encryption.
* Implement differential privacy techniques to add noise to individual data points, making it challenging to single out specific individuals.
* Regular audit and compliance check.
* Privacy-Preserving Machine Learning like federated learning and secure enclaves, or other artificial intelligence and machine learning are used to detect patterns and anomalies associate with cyber threats.

**Techniques for collaboration**

* Collaborative incident response platforms.
* Secure information sharing platform.
* Automated orchestration and response platforms.

## Insider Trading Investigation:

### Scenarios:

Suspicious trading activities across various financial markets is monitored and detected by government or financial institutions, which requires to work with stock exchange, law enforcement agencies for further investigation.

### Blockers

* Legal restrictions and limitation access for non-public information.
* Anonymous trading and use of nominees.
* Reputation damage or unexpected disclosure of non-public information.
* Due to large volumes of trading data, identifying genuine instances of insider trading are resulted false positives investigation and market noise can be a significant challenge.
* It’s difficult to prove individual intention of insider trading.

### Privacy concerns

* Personal information protection.
* Balancing the need of information including financial transactions, communications and personal information is to avoid undue intrusion.
* Third party privacy protection is essential to avoid collateral damage.
* Cross board privacy issue due to legal and regulatory restrictions or data protection standards.

### Techniques for privacy concerns

* Privacy-preserving analytics platforms that allow for the analysis of encrypted or anonymized data.
* Blockchain technology to decentralize and cryptograph the data without impacting for its integrity.
* Encrypted communication platform.
* Mask sensitive information or replace it with tokens to protect personally identifiable information (“PII”) during data analysis.
* Artificial intelligence or machine learning algorithms to anonymize or deidentify sensitive information in datasets.

### Techniques for collaboration

* Secure information sharing platforms.
* Blockchain technology which can enhance collaboration by providing a shared, immutable ledger of transactions and evidence, fostering trust among multiple parties.
* Facilitate seamless integration between different cybersecurity and financial crime investigation tools using APIs.

# Cross-Border Payment Fraud:

### Scenarios:

Fraudulent transaction involving cross boarder payments, which requires bank to work with counter parties’ bank, other financial institutions, international payment networks agencies, regulatory bodies, governments, and law agencies across different countries for further investigation.

### Blockers

* Stringent data privacy regulations. Some countries may have restrictions on the sharing of financial data or may be hesitant to collaborate due to concerns about national security or sovereignty.
* Differences in technology infrastructure and capabilities among countries may impede the harmonized use of advanced analytics and forensic tools in investigations.
* Lack of effective cross-border collaboration mechanisms across complex jurisdictions.
* Fraudsters continuously adapt their methods, making it challenging for investigators to keep pace and develop effective countermeasures.

### Privacy concerns

* Data collecting, processing and sharing will have to adhere with countries data protection regulations.
* Transferring personal data across borders may raise concerns about whether the destination country provides an adequate level of data protection.
* Balancing anonymity with investigation needs.
* Creating clear protocols for cross-border information sharing are essential. These protocols should outline how data will be handled, shared, stored, retained, and protected to address privacy concerns and ensure legal compliance.
* Potential privacy risks for cross boarder sharing, especially for sensitive financial information.

### Techniques for privacy concerns

* Homomorphic encryption.
* Tokenization.
* Privacy-Preserving Analytics Platforms
* Adopt a variety of privacy enhancing technologies, such as k-anonymity, l-diversity, and t-closeness, to anonymize and protect individual transaction data.
* Federated learning or secure enclaves allows collaborative analysis without exposing sensitive information.

**Techniques for collaboration**

* Formalized data sharing agreements and platforms.
* Standardized communication protocols.
* Implement secure identity verification systems that allows collaborators to validate the identities of individuals involved in cross-border transactions without compromising privacy.
* Conduct virtual meetings securely using encrypted video conferencing tools.

## Supply Chain Financing Fraud:

### Scenarios:

Fraudulent activities are identified in supply chain financing arrangements involving multiple businesses and financial institutions, which would require transaction data, supplier information, risk assessments to be shared with involved investigation parties like regulatory bodies, law enforcement agencies and impacted businesses.

### Blockers

* Complexity of supply chain networks.
* Fraudsters might manipulate invoices by inflating amounts, creating fictitious transactions, or altering payment details.
* Operating across borders introduces complexities related to differing legal systems, regulatory frameworks, and cultural nuances, making it challenging to establish uniform anti-fraud measures.
* Lack of collaboration and information sharing among supply chain participants due to competitive issue.

### Privacy concerns

* Supply chain finance transactions often involve the collection and processing of personal information of individuals, including employees, suppliers, and clients. Unauthorized access or breaches can lead to the exposure of sensitive personal data.
* Exposure of confidential business information.
* Supply chain finance often involves collaboration with 3rd party service providers. Inadequate security measures by these entities can pose privacy risks, especially if they have access to sensitive information.
* Inadequate data protection measures.

### Techniques for privacy concerns

* Blockchain for secure and transparent record-keeping.
* Mask or redact sensitive information, ensuring that only authorized individuals have access to the complete data while protecting privacy.
* Utilize robust encryption algorithms to protect data during transmission and storage, ensuring that sensitive information remains confidential and secure.
* Homomorphic encryption.
* Tokenization.

### Techniques for collaboration

* Defining and adopting standardized protocols are required for reporting and sharing information about potential fraud incidents. This ensures consistency and clarity in communication among stakeholders.
* Collaborate with relevant regulatory bodies to share information, align practices, and seek guidance on compliance.
* Utilize encrypted and secure communication channels are encouraged for discussions, regular updates and finance information sharing among stakeholders.

## Terrorist Financing Investigation:

### Scenarios:

Financial transactions with links to potential terrorist financing for terrorists or terrorist organizations are identified across various banks. Regulatory bodies will require transaction data, customer profiles, and intelligence reports to be shared to investigate and disrupt terrorist financing activities with intelligence agencies, international organizations and police.

### Blockers

* Terrorist financiers adapt quickly to changing circumstances, adopting new technologies and tactics. This agility makes it challenging for investigators to stay ahead and anticipate emerging threats.
* Terrorist financing often involves intricate global networks with multiple layers of transactions and funding sources.
* Terrorist financiers may exploit informal and unregulated financial systems, such as hawala networks, to transfer funds discreetly.
* Terrorist financing often involves moving funds across borders, taking advantage of differences in regulatory regimes and enforcement capabilities.
* Some financial institutions might not fully comply with reporting requirements or may underreport suspicious transactions due to concerns about reputation damage or regulatory scrutiny.

### Privacy concerns

* Financial institutions may be required to share transaction data and customer information with law enforcement agencies during terrorist financing investigations. The indiscriminate sharing of such information without proper safeguards can lead to privacy violations.
* The analysis of financial transactions may involve profiling individuals based on their financial behaviour. Innocent individuals could be subject to unwarranted surveillance and scrutiny, impacting their privacy rights.
* International cooperation in terrorist financing investigations may involve sharing financial data across borders. The lack of standardized privacy protections and differing legal frameworks can create challenges and risks for individuals' privacy.
* To protect privacy, investigators often anonymize personal information. However, inadequate anonymization techniques may fail to sufficiently safeguard individuals' identities, leading to potential privacy breaches.

### Techniques for privacy concerns

* Employ robust anonymization and pseudonymization methods to protect the identities of individuals involved in financial transactions. This helps safeguard privacy while allowing for effective analysis of patterns.
* Encrypt sensitive data during transmission and storage to protect it from unauthorized access. Encryption enhances the security of financial information while maintaining privacy.
* Ensure that automated systems used for transaction monitoring and analysis have human oversight to minimize the risk of false positives and prevent unwarranted privacy intrusions.

### Techniques for collaboration

* Develop encrypted and secure platforms that allow for the exchange of information among participating agencies. These platforms should adhere to data protection standards while enabling real-time collaboration.
* Form formal agreements between countries or regions to facilitate cross-border cooperation in terrorist financing investigations. These agreements should outline protocols for information sharing, joint operations, and legal cooperation.
* Utilize MLATs to formalize legal cooperation between countries. These treaties facilitate the exchange of information, evidence, and legal assistance in terrorist financing investigations.

## Identity Theft Ring:

### Scenarios:

Financial institutions identify financial transaction using stolen personal information, and will work with regulatory bodies, credit reporting agencies, and government for identity data, account information, and fraud alerts to dismantle the identity theft ring.

### Blockers

* Identity theft rings often leverage the anonymity provided by the dark web for the exchange of stolen personal information and the sale of compromised identities, making it difficult for investigators to track their activities.
* Use of sophisticated techniques, such as social engineering, phishing, and hacking, making it difficult for investigators to trace and attribute fraudulent activities to specific individuals or groups.
* Identity theft rings frequently exploit data breaches to access large datasets of personal information.
* Identity theft rings increasingly use digital currencies for transactions, enhancing anonymity. Investigating and tracing digital currency transactions pose additional challenges for authorities.

### Privacy concerns

* Unauthorized access to individuals' personal information.
* Data security and protection.
* Data retention periods.
* Inadequate anonymization.
* Limited public awareness.

### Techniques for privacy concerns

* Investigate and adopt technologies that enhance privacy, such as differential privacy or secure multi-party computation, to protect individuals' information while still allowing for effective analysis.
* Access restriction technology.
* Implement strong encryption measures for sensitive personal information to protect it from unauthorized access. Encryption enhances data security and minimizes the risk of privacy breaches.
* Artificial intelligence and machine learning predictive analysis to forecast potential identity theft activities based on historical data and patterns.

### Techniques for collaboration

* Secured information sharing platform and communication channels.
* Centralized databases that can be accessed and updated by multiple agencies. Shared intelligence databases enhance information availability and coordination.
* Develop standardized information sharing protocols.

## Conclusion

In conclusion, as financial crime investigations always involve confidential or sensitive information like personal information and financial records, it’s required for higher standards of ethical considerations while collecting, storing and analysing shared information. Moreover, it also requires advance technology to protect or assist in minimizing privacy concerns for investigations.

From scenarios analysis above, it’s recommended to clearly identify the scope of the data collection, level of data accessing, retention policies and minimize the collection of confidential information. while the information is shared with other parties, it’s required to anonymise the confidential or sensitive information without impact further analysing.

From project/ development point of view, there are 3 main directions from the above analysis.

* Centralized information sharing platform development that can be accessed and updated by multiple agencies, involving privacy impact assessments tool, blockchain technology of cryptographic techniques, encryption techniques like homomorphic encryption, tokenization, symmetric encryption, asymmetric encryption and etc.

PEXA is one real life example for secured digital settlement tool which allow for electronic lodgement of documents and secure payment of settlement. It allows multiple parties including conveyancer, lawyer, bank or financial institution and Land Office to access or exchange documents and complete transaction via platform.

Another example is open banking in Australia, which is initialled by Australia Government in 2018. It will allow customer to give permission to access their personal information, account, production information and transaction records by accredited 3rd parties under the ACCC. Customer will have more controls over how data is used and whom is given. Once permission is granted by customer, their data listed above will be transmitted to 3rd party via open banking.

* Application development with artificial intelligence or machine learning for financial crime investigation or provide alert to organization (similar product like Oracle Financial Services Analytical Applications & BAE system-NetReveal).

1. Supervised and unsupervised machine learning like decision trees and SVMs for historical data analysis of potential patterns or outliers.
2. Neural networks for complex pattern recognition like image, email, communication and speech analysis.
3. Clustering algorithms for patterns and trends of financial data.
4. Federated learning for decentralised or local host data.
5. Behaviours analysis to detect bias and deviation from normal patterns, and fraud score analysis.

* Anonymization product tool development for financial crime investigations (similar product like Privitar & IBM Guardium Data Masking).

Based on current market research and demand of specific areas, DataBytes and their senior management team will decide the direction for our new product and service in the future, which provides a safer, easier and more effective solution to their customers.

## References:

Fargher I (2019) How Westpac is alleged to have broken anti-money laundering laws 23 million times. The Conversation, 25 November 1-4. Accessed on 17th November 2023. <https://ro.uow.edu.au/gsbpapers/582/>.

Gilsinan, J.F., Millar, J., Seitz, N., Fisher, J., Harshman, E., Islam, M. and Yeager, F. (2008) *The role of private sector organizations in the control and policing of serious financial crime and abuse*, Journal of Financial Crime, Vol. 15 No. 2, pp. 111-123. Accessed on 19th November 2023. <https://doi.org/10.1108/13590790810866854>.

Minto, A. and Skovmand Rasmussen, N. (2022) *Approaching the Danske Bank Scandal in a “Tragedy of the Commons” Perspective: Implications for Anti-Money Laundering Institutional Design and Regulatory Reforms in Europe*, European Company and Financial Law Review, Vol. 19 (Issue 2), pp. 305-338. Accessed on 22nd November 2023. <https://doi.org/10.1515/ecfr-2022-0010>.

Nicholls J, Kuppa A and N Le-Khac(2021) *Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape*, IEEE Access, vol. 9, pp. 163965-163986. Accessed on 19th November 2023. <https://ieeexplore.ieee.org/abstract/document/9642993>.

Tipalti(n.d.). *The Total Guide to Cross-Border Payments*. Accessed on 4th December 2023. https://tipalti.com/cross-border-payments-guide/.

Wronka, C. (2023), *Financial crime in the decentralized finance ecosystem: new challenges for compliance*, Journal of Financial Crime, Vol. 30 No. 1, pp. 97-113. Viewed on 20th November 2023. <https://doi.org/10.1108/JFC-09-2021-0218>.