Australia unveils world-first ‘privacy preserving’ fintel encryption project

By Nathan Lynch, Thomson Reuters

Australia’s financial intelligence agency has lifted the bonnet on one of its most ambitious technical projects, which could allow money laundering networks to be uncovered that were previously hidden in the shadows and concealed across multiple banks.

The agency is working on a privacy-preserving encryption system that would enable the Australian Transaction Reports and Analysis Centre (AUSTRAC) to examine patterns in bank data without “seeing” the underlying information.

The ground-breaking work aims to resolve the privacy issues that have hampered the progress of the Fintel Alliance, the country’s public-private financial intelligence partnership. The plan is for banks and regulators to be able to map transactions and relationships to known suspicious accounts across various encrypted data pools without “unpacking” all the underlying data.

Technology experts have viewed homomorphic encryption and other privacy enhancing technologies (PETs) as a possible “holy grail” in the anti-money laundering and counter-terrorism financing (AML/CTF) space. They may solve the challenge of tracing customer transactions across reporting entities, across sectors and even across borders, where privacy or trust are obstacles to greater sharing.
Australien has been quietly exploring this area of cutting-edge encryption technology for more than four years. The project ramped up in earnest one year ago as part of an A$28.4 million budget grant from the federal government. It is financed to continue for another three years through the Fintel Alliance, which is the first such partnership to bring bank staff inside the FIU.

The “Fintel Alliance Alerting Project”, as it is known, will enable alliance members to identify links between suspicious accounts across multiple financial institutions. If the project succeeds, AUSTRAC may be able to scan more than 100 million accounts looking for associates and patterns.

The agency’s complex algorithms would trace financial flows via encrypted bank data (such as the transaction date and time, BSB and account numbers, transaction amounts and transaction descriptions) without ever accessing or “seeing” the decrypted data.

The recent move to the National Payments Platform (NPP) has given Australian banks richer data to link transactions across banks, including through mobile numbers, email addresses and customers’ narrative descriptions. Over time, banks and the FIU may be able to use all of this data to analyse complex transactions across institutions.

THE SECRET TO PRIVACY

The insight into AUSTRAC’s technology is contained in a new report from the Future of Financial Intelligence Sharing (FFIS) project, which promotes the use of public-private partnerships to fight serious and organised crime. The discussion paper, entitled ‘Case studies of the use of privacy preserving analysis to tackle financial crime’, was written by Nick Maxwell, global head of the FFIS program.

“Criminals operate easily across banks. The ability to track them is undermined by the relevant data being held in silos across all the different banks,” Maxwell said.

Maxwell said using privacy-preserving technology was like being able to reveal insights about data held in a safe without ever opening it, and without seeing its contents.

Privacy-preserving analytics can allow “pre-defined queries and macro analysis” to take place on encrypted financial data “without the safe ever being opened.”

“In the past, you had to decrypt all the contents of the ‘safe’ and centralise it to do any analysis on it. You don’t have to do that with PETs,” Maxwell said.

“You can learn from data across different institutions and only
learn things that you are authorised to learn, keeping the rest of the information safe and undisclosed.”

DELVING INTO HIDDEN DATA

Privacy preserving cryptography has been conceived — in theory at least — since the 1970s. It was only in the past decade, however, that computer processing power and cryptography progressed to the point where proponents have been able to launch real-world projects. Some of the early applications include the Zcash cryptocurrency, which relies on “zero knowledge proofs”, and the Enveil ZeroReveal Inter-Bank Secure and Private Data Collaboration project.

The AUSTRAC project is still in the “discovery” phase, but promises to use privacy-preserving technology to reshape the way that banks and intelligence teams investigate financial data.

The UK Financial Conduct Authority is also exploring the potential of this new technology. It ran a “techsprint” last year that focused on the use of PET to tackle financial crime. More than 140 participants took part in the week-long project.

Policymakers, supervisors, FIUs and private sector stakeholders have a unique opportunity to shape and harness this new technology in the AML/CTF space, Maxwell said. The over-arching goal is to fight financial crime by sharing data in a way that is “compliant with regulatory principles, appropriately protects the privacy of individuals and safeguards the confidentiality of business processes.”

VISION FOR INNOVATION

Australia has been quietly leading the charge in this field since 2016. Maria Milosavljevic, AUSTRAC’s chief innovation officer at the time, had a vision for the role that PET could play in solving complex financial crime challenges and sharing critical intelligence. Milosavljevic had led a team that applied similar techniques in a major project at the Australian Crime Commission. Before that federated databases had been used in the Capital Markets CRC (now RoZetta Technology) to detect anomalous stock market activity across borders.

Milosavljevic saw the potential to run AML/CTF analytics at an FIU level without the need to bring all the data into the same place.

“The potential to apply consistent algorithms in a distributed way reduces the risks associated with privacy and security, and addresses some of the barriers to data sharing without compromising privacy. This results in a more precise or surgical approach to identifying suspicious activity,” she said.

The establishment of a PET innovation hub at AUSTRAC has been a gradual but deliberate process. It began four years ago when Milosavljevic lured Kee Siong Ng, a leading authority on PET, from Singapore to Canberra with the promise of working on a confidential and cutting-edge “fintel” project.

Milosavljevic was fortunate that Australia had a top-notch homomorphic encryption (HE) team nearby at the CSIRO’s Data61 lab. The national science agency has been supporting AUSTRAC’s work through its own world-leading research into the application of PET.

Data61 (whose parent organisation, CSIRO has a track record of inventing indispensable things such as wi-fi and polymer bank notes) is a strong proponent of homomorphic encryption. Its researchers have proven that HE can execute calculations that are identical to the results processed “in the clear”, or in an unencrypted state.

“Our Confidential Computing platform enables the analysis of device data without disclosing the data to anyone,” Data61 said. “There is no loss of accuracy due to the encryption process.”

“[Privacy enhancing technology] addresses some of the barriers to data sharing without compromising privacy. This results in a more precise or surgical approach to identifying suspicious activity.”

The security, privacy and accuracy offered by PET will be crucial in improving the analysis and sharing of financial intelligence, Milosavljevic said.

“Not only do new data technologies improve the precision of intelligence. They also offer a game-changing opportunity to shift from traditional regulatory approaches which are often limited to government pre-defining rules and testing compliance, to a world where government works collaboratively with others to leverage leading-edge
technology and genuinely co-regulate,” she said.

At present, tracing transactions across multiple institutions is a slow and cumbersome process. AUSTRAC needs to issue “Section 167” information requests each time it tracks a transaction to a new reporting entity. Criminals exploit this vulnerability by layering transactions across institutions. With the click of a mouse they can hamper an investigation and obscure the big picture that “fintel” analysts are seeking to build.

If successful, AUSTRAC’s project will allow it to map out suspicious funds as they move between accounts and across financial institutions in Australia. In theory, this network could even be extended to participating financial institutions and FIUs overseas.

“The use of privacy enhancing technologies is a key focus of the project and is being deployed to protect the privacy of data relating to innocent customers, including their personal details, accounts and transactions,” AUSTRAC said.

The agency stressed that customer, account and transaction information would not be exposed through the results of the PET algorithms. Instead, the technology will be used to flag accounts that warrant further inquiry.

The power of PET is that it can tell AUSTRAC analysts precisely where the eyes of the needles are hiding, within a “haystack” of nation-wide transaction data.

When a transaction matches a pre-determined criminal typology, AUSTRAC will initiate a follow-up process with the relevant banks. This will be done through formal notices to the financial institutions — in line with the protections and restrictions set out in the AML/CTF Act.

Financial crime specialists said the technology could prove to be a game changer if the pilot study leads to a viable solution — in a production environment — for AUSTRAC. If this is the case other countries are likely to follow suit, possibly with licence-free versions of the AUSTRAC solution. This has happened in the past with AUSTRAC’s original FIU software and later with the “FIU in a Cloud” initiative. The Australian AML/CTF agency has a strong “capacity building” program across the Indo-Pacific region, particularly through its collaborative counter-terrorism work.

Neil Jeans, principal consultant at Initialism in Melbourne, said the technology could provide the same level of insight into domestic transactions that is available for cross-border transactions. The international funds transfer instruction (IFTI) regime requires all cross-border transactions to be reported to AUSTRAC, which allows the FIU to run analytics across the entire data set.
“The approach appears to have carefully considered the privacy implications and addressed them in a way that provides a balance between privacy and the policy objectives to fight serious and organised crime, which other jurisdictions have struggled with,” Jeans said.

Gavin Coles, a financial crime specialist at Kasker Consulting in Melbourne, said the technology held great promise but judicial control over the subsequent production of identifying data would be vital. The tool could also be used to facilitate more civil “proceeds of crime” seizures, he said.

“If you speak to many federal and state level financial investigators, I would suggest that the problem is not identifying who holds and uses criminal assets in Australia, but the failure to act to take those assets off them. Ensuring that there is a real outcome in terms of more dollars or properties seized should be a key priority for the government around all such schemes,” Coles said.

TARGETED INTELLIGENCE GATHERING

At this stage, the project is focused on domestic retail banking transactions and information sharing between the major banks and government partner agencies.

The project will be structured using a “federated” database architecture. This means reporting entities and other participants will engage in the project through an application programming interface (API). When the system generates an alert, AUSTRAC analysts will pick it up and begin the investigation process.

This approach is expected to give AUSTRAC’s analysts the ability to discover criminal networks from the encrypted information of more than 100 million accounts, without revealing any details about the accounts themselves.

“Unlike IFTIs, domestic transactions are not automatically reported to AUSTRAC under Australian legislation and therefore represent an intelligence gap to the agency and our government partners,” AUSTRAC said.

A NEW ERA FOR FINTEL

The coming decade will see a surge in the use of PET technologies in the financial crime space. Despite the promise of these early projects, however, significant hurdles remain in the field. Experts warned that there is a long road to travel between a proof-of-concept and a live production environment. Some of the hurdles are quite mundane, such as ensuring the underlying data is well structured and accurate.

“At the technical level, data quality and data interoperability remain a key concern,” Maxwell said.

The legacy IT systems used in many retail banks are also an obstacle to more advanced technology projects such as this one. As numerous case studies have shown, it is difficult for even the banks themselves to get a single view of the customer across all their business lines. As always, the IT aphorism of “garbage in, garbage out” applies to these types of advanced PET projects.

Leanne Fry, AUSTRAC’s chief innovation officer, said the agency was moving forward carefully with the importance of customers’ privacy foremost in mind.

“The research-intensive capability we are developing will preserve the privacy of citizens’ data, while dramatically increasing our ability to detect criminal behaviour and protect Australia’s financial system and the community from harm.”

“Delivering a world-first project of this nature is an ambitious endeavour. The research-intensive capability we are developing will preserve the privacy of citizens’ data, while dramatically increasing our ability to detect criminal behaviour and protect Australia’s financial system and the community from harm,” Fry said.

Despite the many challenges, the “holy grail” for AUSTRAC and its domestic and international partners is clear. If this research leads to a viable product, FIUs will be able to make further enquiries into suspicious accounts without probing unnecessarily into the activities of legitimate customers. In doing so, they will be able to build a rich, interconnected financial crime intelligence picture in close to real time.

When all is said and done, that will allow AUSTRAC’s partner agencies to detect and disrupt criminal activity at a level of speed and accuracy that was unthinkable in a world before privacy-preserving encryption.
THOMSON REUTERS
REGULATORY INTELLIGENCE

NAVIGATE THE GLOBAL REGULATORY LANDSCAPE WITH CONFIDENCE

Thomson Reuters Regulatory Intelligence delivers a focused view of the global regulatory environment, empowering compliance professionals to make well-informed decisions to manage regulatory risk using the most comprehensive and trusted intelligence available.

This solution cuts through the complexity and sheer volume of content within the regulatory environment by providing clarity on what is most important for your organization, in a cost-effective way.

• A full and up-to-date view of the regulatory environment, from the broadest global industry perspective down to the most granular detail.

• Coverage of over 750 regulatory bodies and over 2,500 rulebooks from across the world – more than anyone else.

• Richest source of regulatory content: news, analysis, rulebooks, regulatory events and practical guidance.

• Actionable and practical information, from board level reporting to operational compliance management.

LEARN MORE AT LEGAL.TR.COM/REGULATORY-INTELLIGENCE