Australian Government

AUSTRAC

AUSTRAC submission

Discussion paper: Reform of Australia's electronic surveillance framework

January 2022

OFFICIAL

Introduction

1. The Australian Transaction Reports and Analysis Centre (AUSTRAC) welcomes the opportunity to provide a submission in response to the *Reform of Australia's electronic surveillance framework* discussion paper.

About AUSTRAC

2. AUSTRAC holds a unique position as Australia's combined anti-money laundering and counter-terrorism financing (AML/CTF) regulator and financial intelligence unit (FIU). We regulate more than 16,000 businesses, which provide services that are vulnerable to money laundering (ML) and terrorism financing (TF) risks, hardening them against misuse and exploitation by criminals. We collect reports from these entities about the movement of money and unusual or suspicious matters. Our data holdings and financial intelligence form a critical component of the national security architecture used to preserve the integrity of Australia's financial system. These holdings are vital in identifying new and emerging risks and aiding law enforcement and security outcomes.
3. AUSTRAC is one of the 10 members of Australia's National Intelligence Community, forming part of a wider group of Commonwealth law enforcement and national security intelligence agencies that work together to protect Australia's interests and national security priorities. In this context, AUSTRAC functions as Australia's specialist FIU, producing actionable financial intelligence to enable other agencies to more effectively achieve their mandates. We also work closely and share our intelligence and expertise with a wide range of domestic and international stakeholders in the public and private sectors.
4. ML is a key enabler of organised crime, allowing criminals to enjoy the profits of crimes such as drug trafficking, tax evasion, people smuggling, theft and fraud, without raising suspicion. Every day, criminals around the world are generating billions of dollars in profits from serious, organised and transnational crime. ML is the process used to place these funds into the legitimate financial system and obscure their origins.
5. The activities of serious, organised and transnational crime groups have significant impacts on Australia and Australians. The Australian Criminal Intelligence Commission estimated serious and organised crime in Australia cost up to $47.4 billion in the 2016–17 financial year.[1] This includes $31.5 billion as the direct and consequential cost of serious organised criminal activity, and $15.9 billion spent on prevention and response to these activities. There are also indirect security, economic and social impacts that make the true cost to Australians far greater.
6. AUSTRAC's submission in response to the discussion paper on the reform of Australia's electronic surveillance framework focuses on:
    a. Part 1: Who can access information under the new framework?

[1] Estimating the costs of serious and organised crime in Australia 2016–17, Australian Institute of Criminology (aic.gov.au). Statistics to be updated in 2022.

b. Part 2: What information can be accessed?
c. Part 3: How can information be accessed?
d. Part 4: When will information be accessed?

Part 1: Who can access information under the new framework?

7. The discussion paper notes that the *Report of the Comprehensive Review of the Legal Framework of the National Intelligence Community* (Comprehensive Review) recommended that AUSTRAC should be permitted to access telecommunications data in its own right under arrangements consistent with other Commonwealth, state and territory law enforcement agencies presently authorised to access telecommunications data.[2]
8. The Government agreed to this recommendation.[3]
9. The inclusion of AUSTRAC as part of the reforms to Australia's electronic surveillance to access telecommunications data will enable the agency to enhance our financial intelligence functions, ensuring we are able to keep pace with rapid evolutions in technology and new payment methods. Customers, both legitimate and criminal, have embraced mobile and internet banking and new payment models, including online money transfer platforms. Telecommunications information will complement and enhance AUSTRAC's traditional transaction reporting data and shed light on potentially illicit transfers using these new payment methods.
10. Having the ability to combine the intelligence generated by transaction and suspicious matter reports with telecommunications data, would provide AUSTRAC and our partner agencies with greater insights into financial and other crimes. Such access would enable earlier identification of suspicious money movements, criminal activity and emerging ML/TF methodologies and risks. It would allow AUSTRAC to produce actionable financial intelligence products that identify connections between entities and transactions before they are provided to law enforcement agencies—rather than relying on the recipient agency, with fewer expert financial analysts, to produce that analysis. It would also bring AUSTRAC into line with regulators such as the Australian Securities and Investments Commission and the Australian Competition and Consumer Commission, who already have this access to telecommunications data.
11. In addition to developing and disseminating actionable financial intelligence products to our domestic partners and international counterparts, AUSTRAC also performs an important role in the provision of financial intelligence that supports interagency investigations and task forces, such as the Serious Financial Crime Task Force, the Illicit Tobacco Task Force, and Australian Federal Police-led Operation Ironside. The ability for AUSTRAC to access telecommunications information to support these task force activities would significantly enhance the quality of AUSTRAC's contributions to intelligence, national security, law enforcement and revenue protection operations.

[2] Recommendation 77.
[3] Commonwealth of Australia, *Government response to the Comprehensive Review of the Legal Framework of the National Intelligence Community, 2020*.

Part 2: What information can be accessed?

12. In accordance with Recommendation 77 of the *Report of the Comprehensive Review of the Legal Framework of the National Intelligence Community*, AUSTRAC seeks the legislative authority to access, on its own initiative, telecommunications data ('non-content' information), which is information about a communication. This could include:
    a. a person's subscriber or account details, such as the phone number or internet protocol address assigned to their service, as well as a person's address and contact details
    b. data associated with communications sent or received by a person, including the date and time of the communication, the participants in a call, and in the case of mobile services, records of which cell tower a device has connected to, which can provide information about the location of the device.
13. This information can provide a range of insights concerning the conduct of financial transactions that may not be apparent from a financial transaction report or information held by a reporting entity. For example, it could enable AUSTRAC to identify the true source of the funds, and the persons who beneficially control the transaction and the true destination of the funds. This information is critical in identifying offences involving transnational, serious and organised crime or TF, where efforts are made to disguise the source and true 'ownership' of the funds.
14. AUSTRAC access to telecommunications data would extend the agency's powers in a relatively limited way, which is proportionate to the benefits that would be achieved for serious financial crime investigations.

Part 3: How can information be accessed?

15. AUSTRAC is seeking access to telecommunications data for the purpose of fulfilling our financial intelligence and regulatory roles to prevent criminal abuse of the financial system and organised crime, including ML and TF.
16. Access to telecommunications data, by AUSTRAC in its own right, is likely to lead to substantially improved AML/CTF outcomes. Direct access to telecommunications data will mean that AUSTRAC's access is not limited to what is shared with AUSTRAC by other agencies, and will enable AUSTRAC to produce enhanced financial intelligence products that support other law enforcement agencies' investigations.
17. AUSTRAC seeks access to telecommunications data under the new electronic surveillance framework. This would reduce the interagency reliance for access to telecommunications data and streamline the process for AUSTRAC to perform our functions.
    a. AUSTRAC is not seeking the legislative authority under the framework to apply for warrants and authorisations to collect and use electronic surveillance ('content' information) on our own initiative.
    b. AUSTRAC, as an important member of many interagency investigations and task forces, should continue to be able to receive 'content' information from eligible agencies, to provide specialist financial intelligence support related to the primary purpose for which the information was collected. This will allow AUSTRAC to continue to support our partners to achieve greater operational outcomes.
    c. AUSTRAC seeks the legislative authority to receive and use lawfully collected 'content' and 'non-content' information for investigations and enforcement action in support of our regulatory and financial intelligence functions. The information must be disclosed to AUSTRAC by an eligible agency under a permitted secondary purpose.
18. With established intelligence and regulatory functions, AUSTRAC has the ability to handle sensitive information data with discretion and in line with legislative obligations. This matter is addressed in detail in the final section of this submission.

Part 4: When will information be accessed?

20. Australia, by virtue of its strong economic prosperity, stability of governments and effective application of the rule of law, will likely remain a destination for proceeds of crime. Unfortunately, Australia remains a highly lucrative market for illicit goods and is targeted by transnational criminal networks. Individual wealth remains a target for fraud and cybercrime. The combination of those threats means proceeds of crime will be laundered through Australia's financial system to reach offshore criminal networks.
21. AUSTRAC supports a proportionate and measured response to electronic surveillance reform that is commensurate with threats faced by law enforcement and national security agencies, to target the underlying criminal business models that supports this illicit activity. This has a significant disruptive impact, reduces harm to the community, and minimises the loss of Government revenue. Criminal syndicates rely on generating profit either as an end in itself, or to facilitate further criminal activities. This means the financial system is at major risk of exploitation to launder and move illicit funds.
22. Terrorism and TF remain ongoing threats to Australians at home and abroad. Even small amounts of money placed in the hands of terrorists and terrorist organisations can result in catastrophic outcomes and erode confidence in financial institutions, and ultimately the Australian economy, that inadvertently facilitate this activity.
23. AUSTRAC uses our regulatory and financial intelligence functions to build resilience in the financial system, enabling the collection of reports from our regulated population about financial transactions, which generate financial intelligence to combat and disrupt ML, TF and other serious crime.
24. Given the very limited manner in which AUSTRAC seeks to access telecommunications information, we are limited in our response to Part 4. AUSTRAC does not intend to seek powers for direct access to:
    a. apply for or obtain warrants
    b. intercept communications, access stored communications, access computers or use surveillance devices to access information.
25. Notwithstanding the above, we support development of a framework that harmonises thresholds for functionally equivalent powers. The new framework should allow agencies to use powers against person/s, objects, third parties and groups where appropriate.
26. As detailed in our response to 'Part 2: What information can be accessed?', AUSTRAC seeks legislative authority to access 'non-content' telecommunications data for the purposes of fulfilling our financial intelligence and regulatory functions to prevent ML, TF and other serious crime.
27. As detailed in our response to 'Part 3: How can information be accessed?', AUSTRAC seeks legislative authority to receive and use 'non content' communications information for our own investigations and enforcement action where a permitted secondary purpose allows.

Other information: privacy and confidentiality of AUSTRAC information

28. AUSTRAC collects a range of information to support our complementary roles as Australia's AML/CTF regulator and FIU. This information is collected under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) and other Commonwealth, state and territory legislation.
29. Reporting entities provide information to AUSTRAC under the AML/CTF Act primarily through the reporting of financial transactions and suspicious matters.
30. AUSTRAC's collection, use, analysis and disclosure of personal information engages privacy obligations under the *Privacy Act 1988* (Privacy Act) and Part 11 of the AML/CTF Act. Key obligations include:
    a. AUSTRAC's obligation to comply with the Privacy Act, including the Australian Privacy Principles
    b. the AUSTRAC CEO's obligation to consult with the Information Commissioner and have regard to privacy in the course of discharging the CEO's duties
    c. the AUSTRAC CEO's and all AUSTRAC officers' obligations to handle AUSTRAC information[4] in accordance with strict secrecy and access provisions set out in the AML/CTF Act.
31. Commonwealth, state and territory agencies that the AUSTRAC CEO authorises to access AUSTRAC information must handle that information in accordance with strict secrecy and access provisions under the AML/CTF Act and Australian Privacy Principles.
32. The secrecy and access provisions in Part 11 of the AML/CTF Act regulate access to, and the use and disclosure of, AUSTRAC information, statutory inadmissibility of some types of information, limitations on the use of particular types of information by particular classes of officials, and a statutory bar on compelling production or disclosure of AUSTRAC information in court or tribunal proceedings. These provisions are intended to ensure that the sensitive information under AUSTRAC's control is secure and protected from unauthorised access, use and disclosure.
33. If AUSTRAC is provided access to telecommunications information under the new framework for electronic surveillance, the interface between secrecy and access provisions under the AML/CTF Act and the new framework should be clearly articulated. AUSTRAC officials and other officials entrusted to access AUSTRAC information should be able to readily understand what safeguards, controls and protections apply to AUSTRAC information that includes telecommunications information.
34. AUSTRAC is subject to oversight by the Privacy Act, *Freedom of Information Act 1982*, the Australian Commission for Law Enforcement Integrity, Commonwealth Ombudsman and

[4] Section 5 of the AML/CTF Act.

the Australian National Audit Office. AUSTRAC is also accountable to Parliament via a number of Parliamentary Committees. The Intelligence Oversight and Other Legislation Amendment Bill 2020 (Integrity Measures Bill), currently before the Australian Parliament, includes provision for AUSTRAC to be subject to oversight by the Inspector-General of Intelligence and Security, and Parliamentary Joint Committee on Intelligence and Security.