Justice & International Mission
Uniting Church in Australia
SYNOD OF VICTORIA AND TASMANIA

:

Centre for Theology and Ministry
29 College Crescent
Parkville Victoria
Australia, 3052
Telephone: +61-3-9340 8807
jim@victas.uca.org.au

[redacted]
Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600
E-mail: pjcis@aph.gov.au

Submission by the Synod of Victoria and Tasmania, Uniting Church in Australia to the review of Item 250 of the *National Anti-Corruption Commission (Consequential and Transitional Provisions) Bill 2022*
31 October 2022

The Synod of Victoria and Tasmania, Uniting Church in Australia, welcomes this opportunity to make a submission to the review of Item 250 of the *National Anti-Corruption Commission (Consequential and Transitional Provisions) Bill 2022*. The Synod supports the new National Anti-Corruption Commission (NACC) having the ability to access metadata, stored data and to make use of International Production Orders (IPOs) as tools it needs to be effective in investigating corruption that falls within its mandate. The Synod notes that the Commonwealth Ombudsman would provide oversight to ensure that the NACC does not misuse its powers under the *Telecommunications (Interception and Access) Act 1979* in terms of interception and access to stored and telecommunication data.

The UN Office on Drugs and Crime has stated:[1]

> *There is a growing consensus among governments globally on the role technology can play in the fight and prevention of corruption. Crucially, it allows for the rapid analysis of vast tracts of data to identify potential instances of corruption in areas such as public procurement, asset disclosures, tax records and financial allocations. On the law enforcement side, this can economise resources through smarter and proactive investigative strategies while reducing huge losses of public funds by improving detection, investigation and analysis of corruption.*

The rest of the following submission provides examples of how access to metadata, subscriber data, and stored communications data are often vital to successful investigations into corruption.

ACLEI's previous submissions to the Committee provided examples of the importance of metadata in corruption cases that fell within their jurisdiction.

1. They were able to use metadata to investigate claims that, for more than five years, law enforcement officials had been assisting a business owner to circumvent inspection protocols that had impacted commercial imports of the business owner. As a result of the investigation, a law enforcement official was convicted of several significant corruption-

[1] UNODC Regional Office for Southeast Asia and the Pacific, 'Introduction to the Role of Data Analytics in Anti-Corruption and Fraud', 7 January 2021.

related offences. In addition, two members of the public, who corrupted the law enforcement official, were facing several significant corruption-related charges.[2]

2. Metadata access assisted in investigating a law enforcement official alleged to have been exploiting his position to facilitate the importation of illicit goods into Australia by non-law enforcement associates. As a result of the investigation, a law enforcement official faced several significant corruption-related charges. In addition, a second law enforcement official appeared in court on a single corruption-related charge.[3]
3. Access to metadata and electronic surveillance was used to investigate allegations that a law enforcement official had released information to a member of the public, who had, in turn, passed it to a person of interest in a criminal investigation. A second investigation followed into allegations that the same law enforcement official and a second law enforcement official had misused their positions and agency resources for personal benefit. As a result of the investigation, the (now former) law enforcement official was to appear in court on a corruption-related charge and a non-corruption-related criminal charge. The second law enforcement official resigned from their employment.[4]

The UK Government has provided several case studies demonstrating the need for anti-corruption investigations to access metadata and stored communication data. The case studies included:

- An investigation that exposed medical supply businesses that corruptly attempted to collude in fixing prices in the supply of medical equipment to the National Health Service. An NHS employee was involved in the corrupt activity. Phone records and subscriber data were essential to the investigation;[5]
- An investigation into corruption in contracts for public road building programmes where a criminal cartel fixed bids at inflated prices. The investigation relied on subscriber data and mobile phone metadata to assist in exposing the cartel;[6]
- Phone subscribers and metadata were used to expose a £200,000 insider-enabled invoice fraud against the National Health Service. Five offenders pleaded guilty to conspiracy charges, and a sixth offender pleaded guilty to money-laundering charges. The communication data was vital to proving the extent of the connection between the conspirators to support the criminal prosecution;[7]
- IP subscriber data were vital in investigating fraud and money laundering by two offenders, one of which was the Continuing Care Manager at the NHS Trust. False invoices for over £117,000 for the continuing care of several fictitious patients were created and paid out. Both offenders were convicted and received custodial sentences. The IP login history associated with the e-mail account allowed the investigator to demonstrate that when the subject was out of the country, the fraud continued to be orchestrated from Nigeria. When the offender returned to the UK, the e-mail account was accessed from a connection that was traced back to the offender's home broadband connection;[8] and,
- Details of all handset identifiers associated with a telephone number and telephone data since the phone account was opened were vital to a corruption investigation into the

[2] Australian Commission for Law Enforcement Integrity, 'Supplementary Submission to the Parliamentary Joint Committee on Intelligence and Security. Review of the Mandatory Data Retention Regime', 19 February 2020, 5.
[3] Ibid., 5-6.
[4] Ibid., 6.
[5] UK Home Office, Investigatory Powers Bill: Overarching Documents, 'Operational case for the use of communications data by public authorities', 2017, 16, https://www.gov.uk/government/publications/investigatory-powers-bill-overarching-documents
[6] Ibid., 17.
[7] Ibid., 67.
[8] Ibid., 68

> payment of significant bribes to secure multi-million dollar contracts. Upon arrest, the suspect produced a mobile phone believed to be crucial to the investigation. When forensically examined, the handset contained considerably less information than expected. The offender then failed to comply with a Notice compelling him to produce any further mobile telephones in his possession. Investigators believed the individual had deliberately not produced the actual handsets subject to the Notice in order to conceal incriminating evidence. Communications data accessed by the investigators demonstrated that the offender had swapped a SIM card into a different handset before surrendering it upon arrest. In addition, corroborating evidence was obtained from itemised billing data showing a missing handset and that it had been used pursuant to corrupt activity. The suspect was subsequently charged with concealing evidence on the strength of the accessed communication data.[9]

Exposing the Invisible has provided examples of how accessing metadata can assist in investigations into corruption.[10] Associated Press investigated the use of government funds by US congressman Aaron Schock. They extracted geolocation data from photos Mr Schock posted and tagged along with his location on his Instagram account and then compared it to the travel expenses he claimed as campaign expenses. The photos featured him jumping into snow banks, on sandy beaches and in various private planes. Flight ecords of airport stopovers and the data extracted from his Instagram account found that public and campaign funds had been spent on private plane flights. A US$1,928 invoice paid to the ticket service StubHub.cm to attend a Katy Perry concert was listed as a "fund-raising event" on Mr Schock's expenses. The AP published their findings on 24 February 2015. On 17 March 2015, Mr Schock announced his resignation from Congress.[11]

Anti-corruption agencies in Cambodia, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Thailand and Viet Nam reported that lack of cooperation from organisations that collect data is the most significant problem in being able to apply data analytics to address corruption.[12]

[redacted]
Senior Social Justice Advocate
[redacted]
[redacted]

[9] Ibid., 74.
[10] Exposing the Invisible, ‘Behind the Data: Investigating metadata’, 1 December 2017.
[11] Ibid.
[12] UNODC Regional Office for Southeast Asia and the Pacific, ‘Introduction to the Role of Data Analytics in Anti-Corruption and Fraud’, 7 January 2021.