130 Little Collins Street Melbourne Victoria Australia, 3000

Telephone: +61-3-9251 5271 Facsimile: +61-3-9251 5241 jim@victas.uca.org.au

Data Availability and Use Productivity Commission GPO Box 1428 Canberra City ACT 2601

Submission by the Justice and International Mission Unit, Synod of Victoria and Tasmania, Uniting Church in Australia to the Data Availability and Use Issues Paper 29 July 2016

The Justice and International Mission Unit, Synod of Victoria and Tasmania, Uniting Church in Australia, welcomes this opportunity to make submission to the *Data Availability and Use* Issues Paper.

The Unit will make comments on some of the questions in the Issues Paper as they apply to work the Unit has been doing on issues around tax avoidance, tax evasion, money laundering, human trafficking and forced labour.

What public sector datasets should be considered high-value data to the: business sector; research sector; academics; or the broader community?

What benefits would the community derive from increasing the availability and use of public sector data?

What are the main factors currently stopping government agencies from making their data available?

Customs Data

Australians should be able to be assured that the products they purchase have not been produced with the involvement of serious criminal activity. There is a need to stop crossborder trade being a mechanism by which the proceeds of crime (such as goods produced through the use of slavery, human trafficking, forced labour or other egregious human rights abuses) are laundered before being purchased by consumers. The US Department of Labor produces a list of goods imported into the US that are at risk of having involved forced labour child labour found or in their production, which can be at https://www.dol.gov/ilab/reports/child-labor/list-of-goods/. Many of the same goods from the same countries are also imported into Australia. However, unlike the US where customs data about which companies are importing from where, the Australia Government keeps customs data secret and only allows for the ABS to publish aggregated and de-identified customs data.

Further, despite Division 270 of the Commonwealth *Criminal Code Act 1995* making slavery an offence extraterritorially, no Australian company has ever been prosecuted for the importation of products produced through slavery or human trafficking, as such a prosecution would be near impossible to mount.



Where companies import goods that have been produced through serious criminal activity, such as slavery, forced labour or human trafficking, they are almost certainly able to gain an unfair price advantage over competitors that have produced their products legally. Making customs data public will open importers of products more accountable to ensure the products they are importing have been legally produced, as it would allow third parties and consumers to identify where Australian importers are sourcing from.

Examples of customs data that is publicly available in the US and in India are attached.

Currently the Australian Government captures customs data through the Australian Government's Integrated Cargo System (ICS) and includes details such as the nature and quantity of the product, the supplier and the intended recipient. In other jurisdictions, including the United States, the EU and India, this data is either made publically available directly or is available for purchase from third party data mapping companies. However, import data collected through ICS is only currently available in detail to entities directly involved in importation of the specific product. Limited statistical data from ICS is made also available to the Australian Bureau of Statics for research purposes.

Making key data about imported products publically available would improve the ability of business, civil society and consumers to detect where Australian importers are dealing with suppliers where there is the presence of criminal activity in the production of the goods and the source jurisdiction has failed to take effective action to stop the criminal abuse. This would have a deterrent impact on the risks Australian importers are willing to take in dealing with suppliers where there is significant risk of criminal; activity in the production of the goods, out of concern for reputational risk. It would also assist businesses to verify supply chains. For example, in the US, companies have been able to use import data to monitor the fishing vessels of suppliers in South East Asia.

In the jurisdictions where customs data is publicly available there is no evidence of any significant impact on commercial activities or the proper functioning of markets. There is evidence that it has assisted importers in those jurisdictions to be made aware of risks of criminal activity in relation to suppliers they are sourcing from. The Unit can put the Productivity Commission in touch with relevant staff in the US Department of Homeland Security to explain further how making custom's data public in the US has assisted in addressing criminal activity in the production of goods being imported into the US.

ASIC Company Register and Disclosure of Beneficial Ownership

The Australian Government should update the ASIC company register so that it publicly discloses the ultimate beneficial ownership of companies registered in Australia. In our experience, currently the ASIC database of company ownership has allowed companies to be registered at false addresses. The Fair Work Ombudsman has had a similar experience when it investigated labour hire companies that were supplying workers to Baiada, see https://www.fairwork.gov.au/about-us/news-and-media-releases/2015-media-releases/june-2015/20150618-baiada-group-statement-of-findings

The fees charged by ASIC for accessing information from the company database are also high for anyone wishing to do research across many companies by comparison to accessing similar data in other countries (such as Hong Kong, Singapore and Ireland) and the Unit asks that the Productivity Commission review the fees being charged to access information on the ASIC company register.



Beneficial ownership is defined in the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)*

(see: https://www.legislation.gov.au/Details/F2015C00917).

Under the provisions of the rule a beneficial owner is someone (a natural person, not a legal entity) who owns or controls (directly or indirectly) a business where:

- (a) In this definition: control includes control as a result of, or by means of, trusts, agreements, arrangements, understandings and practices, whether or not having legal or equitable force and whether or not based on legal or equitable rights, and includes exercising control through the capacity to determine decisions about financial and operating policies; and
- (b) In this definition: owns means ownership (either directly or indirectly) of 25% or more of a company.

The current ASIC database needs to remain in public hands. Given that shell companies with hidden ownership are present in facilitating a wide range of serious criminal activity (human trafficking, money laundering, financing terrorism, commercial online child sexual abuse, illicit arms trading, fraud, embezzlement, bribery and tax evasion), as exposed by the Panama Papers (see https://panamapapers.icij.org/20160403-panama-papers-global-overview.html) it is not appropriate that the database of company ownership would be placed in private hands. This should be seem as one of the vital tools for law enforcement and therefore should remain under government control.

Having an accurate, accessible company registry, that includes disclosure of ultimate beneficial ownership would be a great assistance to Australian businesses that have antimoney laundering and countering terrorism financing obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*. Such a registry would reduce the due diligence costs for reporting entities under the Act to determine ultimate beneficial owners of corporate entities they are dealing with and assess money laundering and terrorism financing risks. Costs are also saved by the fact that multiple reporting entities are not paying for the same due diligence as each other, if the beneficial ownership registry is public.

Through the G20 the Australian Government has already promised to deliver on beneficial ownership transparency:

https://www.ag.gov.au/CrimeAndCorruption/AntiCorruption/Documents/G20High-LevelPrinciplesOnBeneficialOwnershipTransparency.pdf

The World Bank and UN Office on Drugs and Crime have stated on the usefulness of registries of beneficial ownership:¹

.... finds that registries can usefully compliment anti-money laundering objectives by implementing minimum standards for the information maintained in the registry and by providing financial institutions and law enforcement authorities with access to adequate, accurate, and timely information on relevant persons connected to corporate vehicles — corporations, trusts, partnerships and limited liability characteristics, foundations and the like.

The UK Government had previously revealed that 6,150 people acted as directors of more than 20 UK registered companies, with some people being directors in over 1,000

_

¹ Kevin Stephenson, Larissa Gray, Ric Power, Jean-Pierre Brun, Gabriele Dunker and Melissa Panjer, 'Barriers to Asset Recovery', The World Bank and UNODC, Washington, 2011, p. 34.



companies, clearly indicating some directors were acting as front people for the ultimate beneficial owners.

A research report by World-Check had previously shown that almost 4,000 people who are appear on various international watch lists are registered as directors of UK companies. This included 154 people allegedly involved in financial crime, 13 individuals wanted by Interpol for alleged terrorist activities and 37 accused of involvement in the drugs trade.

The Panama Papers have provided a small window on the world in which unethical high net worth individuals and multinational corporations use shell companies with concealed ownership to facilitate tax avoidance and tax evasion. Shell companies with concealed ownership are also used as vehicles to facilitate a range of serious criminal activity, from human trafficking, money laundering, financing terrorism, commercial online child sexual abuse, illicit arms trading, fraud, embezzlement and bribery.

The OECD had previously provided data on the use of special purpose entities (SPEs or shell companies) through jurisdictions that have assisted in profit shifting by multinational companies. In general terms, SPEs are entities with no or few employees, little or no physical presence in the host economy, whose assets and liabilities represent investments in or from other countries, and whose core business consists of group financing or holding activities.²

Research by Findley, Nielson and Sharman also found Australian corporate service providers were near the top of corporate service providers in terms of being willing to set up an untraceable shell company even when there was significant risk the company in question would be used for illicit purposes.³

The ATO had publicly stated some time ago "Over a hundred Australians have already been identified involving tens of millions of dollars in suspected tax evasion through the use of 'shell companies' and 'trusts' around the world." In October 2013, the Australian Federal Police charged three men with tax and money laundering offences involving \$30 million. It is alleged they used a complicated network of offshore companies to conduct business in Australia while hiding the profits offshore, untaxed. The profits were then transferred back to Australian companies controlled by the offenders and disguised as loans so the interest could be claimed as a tax deduction. The level of alleged criminal benefit was estimated at \$4.9 million.

The World Bank and UN Office on Drugs and Crime (UNODC) have previously conducted research showing how shell companies with concealed ownership are used to facilitate a range of criminal activity. They published a report reviewing some 150 cases of corruption where the money from laundered. In the majority of cases:⁴

- A corporate vehicle (usually a shell company) was misused to hide the money trail;
- The corporate vehicle in question was a company or corporation;
- The proceeds and instruments of corruption consisted of funds in a bank account; and

² OECD, 'Addressing Base Erosion and Profit Shifting', OECD Publishing, http://dx.doi.org/10.1787/9789264192744-en, 2013, p. 18.

³ Michael Findley, Daniel Nielson and Jason Sharman, 'Global Shell Games: Testing Money Launderers' and Terrorist Financiers' Access to Shell Companies', Centre for Governance and Public Policy, Griffith University, 2012, p. 21.

⁴ Emile van der Does de Willebois, Emily M Halter, Robert A Harrison, Ji Won Park and J. C. Sharman, 'The Puppet Masters', The World Bank, 2011, p. 2.

 In cases where the ownership information was available, the corporate vehicle in question was established or managed by a professional intermediary to conceal the real ownership.

In two-thirds of the cases some form of surrogate, in ownership or management, was used to increase the opacity of the arrangement.⁵ In half the cases where a company was used to hide the proceeds of corruption, the company was a shell company.⁶ One in seven of the companies misused were operational companies, that is 'front companies'.⁷

As an example of a case where shell companies with concealed ownership were allegedly used to facilitate money laundering through Australia, US authorities sought to seize the assets in three Westpac accounts held by Technocash Ltd holding up to \$36.9 million. Technocash Limited was an Australian registered company. The funds are alleged to be connected to shell companies owned by the defendants in the case. It is unclear if Westpac had detected the connection between Technocash and key figures in Liberty Reserve and their alleged criminal activities, particularly money laundering. According to the case filled by the US Attorney for the Southern District of New York, Liberty Reserve SA operated one of the world's most widely used digital currencies. Through its website, the Costa Rican company provided its with what it described as "instant, real-time currency for international commerce", which could be used to "send and receive payments from anyone, anywhere on the globe". The US authorities allege that people behind Liberty Reserve: 10

...intentionally created, structured, and operated Liberty Reserve as a criminal business venture, one designed to help criminals conduct illegal transactions and launder the proceeds of their crimes. Liberty Reserve was designed to attract and maintain a customer base of criminals by, among other things, enabling users to conduct anonymous and untraceable financial transactions.

Liberty Reserve emerged as one of the principal means by which cyber-criminals around the world distributed, stored and laundered the proceeds of their illegal activity. Indeed, Liberty Reserve became a financial hub of the cyber-crime world, facilitating a broad range of online criminal activity, including credit card fraud, identity theft, investment fraud, computer hacking, child pornography, and narcotics trafficking. Virtually all of Liberty Reserve's business derived from suspected criminal activity.

The scope of Liberty Reserve's criminal operations was staggering. Estimated to have had more than one million users worldwide, with more than 200,000 users in the United States, Liberty Reserve processed more than 12 million financial transactions annually, with a combined value of more than \$1.4 billion. Overall, from 2006 to May 2013, Liberty Reserve processed an estimated 55 million separate financial transactions and is believed to have laundered more than \$6 billion in criminal proceeds.

⁵ Emile van der Does de Willebois, Emily M Halter, Robert A Harrison, Ji Won Park and J. C. Sharman, 'The Puppet Masters', The World Bank, 2011, p. 58.

⁶ Emile van der Does de Willebois, Emily M Halter, Robert A Harrison, Ji Won Park and J. C. Sharman, 'The Puppet Masters', The World Bank, 2011, p. 34.

⁷ Emile van der Does de Willebois, Emily M Halter, Robert A Harrison, Ji Won Park and J. C. Sharman, 'The Puppet Masters', The World Bank, 2011, p. 39.

⁸ USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 29, 43.

⁹ USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 21. ¹⁰ US Attorney for the Southern District of New York, 13 Civ 3565, 28 May 2013, pp. 4-5.



It was further alleged by US authorities that for an additional "privacy fee" of 75 cents per transaction, a user could hide their own Liberty Reserve account number when transferring funds, effectively making the transfer completely untraceable, even within Liberty Reserve's already opaque system.¹¹

US authorities alleged defendant Arthur Budovsky used Technocash to receive funds from exchangers. Mr Budovsky, the alleged principal founder of Liberty Reserve, ¹² allegedly used his bank to wire funds to Technocash bank accounts held by Westpac. ¹³ He is also alleged to be the registered agent for Webdata Inc which held an account with SunTrust. Technocash records allegedly showed deposits into the SunTrust account from Technocash accounts associated with Liberty Reserve between April 2010 and November 2012 of more than \$300,000. ¹⁴

Arthur Budovsky is allegedly listed as the president for Worldwide E-commerce Business Sociedad Anonima (WEBSA) and defendant Maxim Chukharev as the secretary. Maxim Chukharev is alleged to have helped design and maintain Liberty Reserve's technological infrastructure. ¹⁵ WEBSA allegedly served to provide information technology support services to Liberty Reserve and to serve as a vehicle for distributing Liberty Reserve profits to Liberty Reserve principals and employees. ¹⁶ It is alleged bank records showed that from July 2010 to January 2013, the WEBSA account in Costa Rica received more than \$590,000 from accounts at Technocash associated with Liberty Reserve. ¹⁷

It is alleged Arthur Budovsky was the president of Grupo Lulu Limitada which was allegedly used to transfer and disguise Liberty Reserve Funds. ¹⁸ Records from Technocash allegedly indicate that from August 2011 to November 2011 a Costa Rican bank account held by Grupo Lulu received more than \$83,000 from accounts at Technocash associated with Liberty Reserve. ¹⁹

Further, defendant Azzeddine El Amine, manager of Liberty Reserve's financial accounts, ²⁰ was the Technocash account holder for Swiftexchanger. It is alleged e-mails showed that exchangers wishing to purchase Liberty Reserve currency wired funds to Swiftexchanger. When Swiftexchanger received funds in its Technocash account, an e-mail alert was sent to

-

¹¹ US Attorney for the Southern District of New York, 13 Civ 3565, 28 May 2013, p. 6.

¹² US Department of Justice, 'One of the World's Largest Digital Currency Companies and Seven of Its Principals and Employees Charged in Manhattan Federal Court and Running Alleged \$6 Billion Money Laundering Scheme', 28 May 2013.

USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 29.
 USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 36.
 US Department of Justice, 'One of the World's Largest Digital Currency Companies and Seven of Its Principals and Employees Charged in Manhattan Federal Court and Running Alleged \$6 Billion

Its Principals and Employees Charged in Manhattan Federal Court and Running Alleged \$6 Billion Money Laundering Scheme', 28 May 2013.

USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 37.
 USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 36.

¹⁷ USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 38.

¹⁸ USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 36.

¹⁸ USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 40.

¹⁹ USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 36. ¹⁹ USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 41.

²⁰ US Department of Justice, 'One of the World's Largest Digital Currency Companies and Seven of Its Principals and Employees Charged in Manhattan Federal Court and Running Alleged \$6 Billion Money Laundering Scheme', 28 May 2013.



El Amine, notifying him of the transfer. Based on these alerts, it is alleged between 12 June 2012 and 1 May 2013, exchangers doing business with Liberty Reserve send approximately \$36,919,884 to accounts held by Technocash at Westpac.²¹

The defendants are alleged to have used Technocash services to transfer funds to nine Liberty Reserve controlled accounts in Cyprus.²²

Technocash Limited is reported to have been forced out of business in Australia following the action by US authorities, when it was denied the ability to establish accounts in Australia by financial institutions. Technocash stated that it "complied with Australia's comprehensive AML regime, verified customers and has an AFSL licence since 2003. Technocash denies any wrong doing."

Dr Mark Zirnsak Director Justice and International Mission Unit

²¹ USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 30. ²² USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 31.

²³ Technocash, 'Opportunity: Own the Technocash Payment Platform', Media Release, 5 July 2013.