Uniting Church in Australia
SYNOD OF VICTORIA AND TASMANIA

Justice and International Mission Unit
130 Little Collins Street
Melbourne Victoria 3000

Committee Secretary
Parliamentary Joint Committee on Law Enforcement
PO Box 6100
Parliament House
Canberra, ACT, 2600
E-mail: le.committee@aph.gov.au

Justice and International Mission Unit
Synod of Victoria and Tasmania, Uniting Church in Australia

Submission to Inquiry into financial related crime
9 May 2014

The Justice and International Mission Unit, Synod of Victoria and Tasmania, Uniting Church in Australia (the Unit) welcomes this opportunity to make a submission into the effectiveness of current Commonwealth law enforcement legislation and arrangements that target serious and organised financial related crime including money laundering.

The Uniting Church in Australia is committed to working for an end to poverty globally and corruption and financially motivated crimes are often barriers to poverty reduction. For example, we have conducted research into politically exposed persons (PEPs in the language used in anti-money laundering legislation) from PNG who have been charged with corruption related offences in PNG and appear to have been able to transfer assets freely into Australia.

In October 2012 Sam Koim, the head of the Papua New Guinea anti-corruption body Taskforce Sweep, publicly stated that Australia had, at that time, never repatriated any funds stolen through corruption to PNG. He went on to allege that corrupt people from PNG:

> *have bought property and other assets, put money in bank accounts and gambled heavily in your casinos and have never been troubled by having their ill-gotten gains taken off them. Unless the money can be prevented from leaving our country or prevented from entering Australia, the bad guys win and the rest of Papua New Guinea suffers.*

He stressed what was at stake:

> *When money that is supposed to build hospitals, to buy medical equipment is used to buy real estate in Cairns or Brisbane, people die. And, quite frankly, those who turn a blind eye to this are as guilty as the offenders.*

He also said:

> *Be under no illusion, these people have chosen Australia as their preferred place to launder and house the proceeds of their crimes because it is easy. Cairns is only a short flight and property can be bought off the plan without permission. The financial*

system is stable and, it has been, up until now, extremely easy to get money into your system….

As Chairman of Taskforce Sweep, I am privy to the thinking of our Prime Minister on this topic. I can share with you the fact he has become increasingly unhappy as our Taskforce has progressed, with the fact that the Australian financial system is being used to systematically launder tens of millions and possibly hundreds of millions of kina that should be used to provide healthcare, education and infrastructure for our people – the priority areas of the Government I represent.

This submission will address the following terms of reference:

- The methods and practices used by the perpetrators of financial related crime (including the impact of new technologies);
- The operation and effectiveness of Commonwealth legislation, administrative arrangements and law enforcement strategies;
- The role of the Australian Crime Commission and the Australian Federal Police in detecting financial related crime;
- The extent and effectiveness of the relevant international agreements and arrangements; and
- The need for any legislative or administrative reform.

Recommendations

The Justice and International Mission Unit requests the Committee make the following recommendations to strengthen Australia's response to financially related crime:

Recovery of Stolen Assets

- The Australian Government should follow the examples of the UK and US Governments and set up a small unit within the Australian Federal Police to identify and return assets stolen from developing countries and shifted into Australia. This could be simply an expansion of the existing Criminal Assets Confiscation Taskforce to include a section that targets assets stolen from developing countries.

Enhancing the Anti-Money Laundering Regime

- AUSTRAC and the Australian Institute of Criminology should carry out more investigation into reporting entities compliance with the AML/CTF legislation and the results of the investigation should be made public so that the Australian community can have a better idea of how well the system is functioning, similar to work that has already been carried out by the UK Financial Service Authority.[1]
- Remove "to affect beneficially Australia's relations with foreign countries" from the objects of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*.
- The following objects should be added to the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006:*
    - To detect and deter money laundering and financing of terrorism and reduce the risk to the integrity of the financial system.
    - To provide officials with information necessary to investigate and prosecute money laundering and financing of terrorism, thereby reducing crime; and
    - To provide Australia's financial intelligence unit and AML/CTF regulator with powers to collect information, supervise reporting entities and enforce AML/CTF regulations.

[1] Financial Service Authority, 'Bank's management of high money-laundering risk situations', June 2011.

- Regulatory authorities need to have a greater 'hands-on' role in ensuring that reporting entities meet both the letter and the intent of the requirements of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*.
- The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* should allow a reporting entity to terminate a relationship with a customer if, after having submitted a suspicious transaction report to AUSTRAC, it has not received any response from AUSTRAC or other authorised office of an authorised agency within seven days. In the UK, the *Proceeds of Crime Act 2002* makes it a money-laundering offence to handle criminally obtained funds, unless an authorised disclosure is made and consent to handle the funds is obtained from the National Crime Authority.[2] The National Crime Authority has seven working days to grant or deny consent to handle the criminally obtained funds.
- The Australian Government should require a thorough evaluation of the impact of the new AUSTRAC rules relating to Politically Exposed Persons and investigation of beneficial ownership after an appropriate time has been allowed for their implementation.
- The Australian Government should implement regulations in line with World Bank recommendations that a public official should be asked to provide a copy of any asset and income declaration form filed with their authorities, as well as subsequent updates. If a customer refuses, the bank should be required to assess the reasons and determine, using a risk-based approach, whether to proceed with the business relationship.
- The Australian Government should also require AUSTRAC rules to be modified, in line with World Bank recommendations, so that where a person has ceased to be entrusted with a prominent public function, there should be no time limits on the length of time the person, family member, or close associate needs to be treated as a PEP.
- The Australian Government should require financial institution to disclose full details of foreign state assets that they manage. In dictatorships where one individual, or a small cabal, exercises almost complete power over the state, there is a very thin dividing line between state and personal investments.
- The Australian Government should implement the FATF recommendation to it to adopt legal requirements for branches and subsidiaries in foreign jurisdictions to apply the higher AML/CTF standard, to the extent that the laws of the host jurisdiction allows. In the event where a foreign branch or subsidiary is unable to observe appropriate AML/CTF measures because this is prohibited by local (i.e. host jurisdiction) laws, regulations or other measures, those financial institutions should be required to inform Australian authorities.
- The Australian Government should add designated non-financial businesses and professions, as defined in the FATF Recommendations, more thoroughly to the AML/CTF regime.
- Australian authorities should automatically share information with authorities of other governments (especially foreign FIUs) when a foreign PEP purchases property in Australia, transfers funds to an Australian bank account or gambles at an Australian casino or other gambling venue, unless the Australian authorities have some reason to carry out a prosecution of the person in question themselves or entities involved in the transaction and the sharing of information would compromise that prosecution. Further, such information should not be shared if the Australian Government has reasonable concerns the information is likely to be used to carry out human rights abuses against the PEP in question. As in the vast majority of cases, Australian authorities would not carry out any investigation or legal action themselves against a foreign PEP in relation to suspicious transactions it is hard to see that anything is lost by automatically sharing the information above with authorities of other governments. Information about property purchases is publicly available anyway, at a small cost.

[2] National Crime Agency, 'Obtaining consent from the NCA under Part 7 of the Proceeds of Crime Act (POCA) 2002 or under Part 3 of the Terrorism Act (TACT) 2000', October 2013.

- The Australian Government should implement the World Bank and UNODC recommendation that when a suspicious transaction report is linked to a foreign PEP, the competent authorities should, after proper analysis supports such dissemination, share this information with the competent authorities in the PEP's home jurisdiction and any other germane jurisdiction.

Public Registry of Company and Trust Ownership

- Given the role of shell companies and trusts with hidden ownership often play in cases of money laundering the Australian Government should introduce legislation to create a public registry of the true ownership of companies and trusts; where these assets are held; and who benefits from them. The UK Government has recently released details of the public register of ultimate beneficial ownership of companies it plans to implement.

Unexplained wealth

- That the Commonwealth Government implement the previous recommendations of the Committee with regards to unexplained wealth legislation and arrangements, especially Recommendation 15 that supported a "national unexplained wealth scheme, where unexplained wealth provisions are not limited by having to prove a predicate offence."[3]
- That the Commonwealth Government ensure that there are in place effective mechanisms that allow for prompt tracing and temporary freezing of criminal assets shifted into Australia from overseas before a formal mutual legal assistance request is filed. A formal mutual legal assistance request should be required to retain the freeze.
- Australia should provide reasons for rejecting any mutual legal assistance request from a foreign jurisdiction relating to recovery of stolen assets to the originating jurisdiction and the originating jurisdiction should be given the opportunity to demonstrate that the defendant received due process.
- That the Commonwealth Government ensure it has an effective non-conviction based confiscation and restraint mechanism to deal with criminal assets transferred from overseas into Australia.

Combatting Online Commercial Child Sexual Abuse

- Extend the requirement for ISPs to disrupt access to child sexual abuse material from the INTERPOL domain list to all child sexual abuse material that is illegal under Australian law. This INTERPOL list only covers child sexual abuse material involving children aged 12 and under. The extension could be possible through working with the UK Internet Watch Foundation given the similarity between Australian and UK law on the definition of 'child pornography'.
- The Australian Government should actively support the UK Government in requiring search engines not to assist offenders by providing search results for child sexual abuse material.
- Fund research into Australian offenders who access child sexual abuse material to identify their pathways to offending and assist in identifying measures to reduce this criminal activity.
- Seek to assist in the commissioning of international research into commercial child sexual abuse operations online, with a view of undermining the ability of these operations to attract customers and make profit where it is not possible to locate and shut down such operations.
- Increase funding for the AFP to increase law enforcement activities against those accessing, trading in and purchasing child sexual abuse material.
- Provide assistance to other countries to harmonise laws criminalising child sexual abuse material online and provide increased technical assistance on law enforcement. This

[3] Parliamentary Joint Committee on Law Enforcement, 'Inquiry into Commonwealth unexplained wealth legislation and arrangements', March 2012, p. xvi.

should include active participation in the Global Alliance against child sexual abuse online, the Virtual Global Taskforce and the International Telecommunications Union Child Online Protection initiative.

- Actively promote where Australians should report inadvertent encounters with child sexual abuse material online to.
- Support the roll out of new technologies, such as Microsoft's Photo DNA, that assist in the removal known images of child sexual abuse material.
- Follow the example of the US Government and introduce a legislative mechanism by which it is possible for victims of child sexual abuse to seek restitution payments from people who have downloaded their images, including the purchasing of the images. In the Us this is done through a provision in the *Violence Against Women Act*.[4]
- Explore catered rehabilitation programs for non-contact offenders where there are sufficient numbers to justify such programs to reduce recidivism.
- Explore the ability to provide a help service for offenders who recognise they have a problem and wish to seek help in ending their offending behaviour. This can be advertised through the 'Stop' message tied to ISP level access disruption.
- Implement the recommendation of the UN Committee on the Rights of the Child from 19 June 2012 to develop and implement a comprehensive and systematic mechanism of data collection, analysis, monitoring and impact assessment of child sexual abuse offences. This should include data collected on the number of prosecutions and convictions, disaggregated by the nature of the offence.
- Ensure that URLs and domains that have been used by commercial child sexual abuse operations are deregistered and cannot be used again.

[4] Emily Bazelon, 'The Price of a Stolen Childhood', *The New York Times*, 24 January 2013.

Table of Contents

1. Theft from Developing Countries

The Unit notes that the World Bank and UN Office on Drugs and Crime (UNODC) believe that $20 to $40 billion a year is lost from developing countries due to corruption (and this excludes money lost by tax evasion by multinational companies), only $5 billion in total has been repatriated to developing countries in the last 15 years.[5] They noted most of the legal barriers are onerous requirements to the provision of mutual legal assistance, a lack of non-conviction based asset confiscation procedures and an overly burdensome procedural and evidentiary laws.[6]

In cases of the theft of assets from governments and cases of corruption, often the only tangible evidence that a crime has taken place is the money that changes hands between the corrupt official and his or her partner in crime. Thus the enrichment of the corrupt official becomes the most visible manifestation of corruption. An offense such as bribery, which requires the demonstration of an offer by the corruptor or acceptance by the official, is difficult to prosecute in these circumstances. Similarly, once an offense has been established in a court of law, linking the proceeds to an offense for the purposes of recovering assets can often be a complex endeavour. Efforts to combat corruption are further challenged by the anonymity and fluidity with which assets can be moved, concealed, and transferred before effective means can be taken to seize, freeze, and return them to their rightful owners.[7]

As noted by Sam Koim above, there is strong evidence that Australia remains a destination for some of the funds stolen from developing country governments.

The Unit rejects the morally bankrupt argument that Australia should not take steps to address money stolen from developing countries being shifted into Australia on the basis that if it did not end up in Australia it would go somewhere else. The implication of such an argument is that the Australian Government should allow some Australian businesses to benefit from crimes committed overseas on the basis that overseas businesses will benefit from the criminal activity so it might as well be Australian businesses. Instead Australia needs to be part of global efforts to limit the boltholes criminals can shift their ill-gotten gains to. Australia has a stable financial system, making it an attractive destination for criminals to transfer assets to if they can be confident they will be able to access them. By Australia participating in global efforts to combat the transfer of criminal assets, it is hoped the remaining boltholes will be higher risk to criminals that they might lose their assets or have them stolen, so as to deter the motivation for the criminal activity.

2. Need for a Specialist Unit on Stolen Asset Recovery

The Australian Government should follow the examples of the UK and US Governments and set up a small unit within the Australian Federal Police to identify and return assets stolen from developing countries and shifted into Australia. This could be simply an expansion of the existing Criminal Assets Confiscation Taskforce to include a section that targets assets stolen from developing countries.

In 2006 a Proceeds of Crime Unit was set up within the Metropolitan Police to investigate such cases. By 2010, the Proceeds of Crime Unit had taken actions resulting in the freezing of £160 million ($296 million) of assets.

---

[5] 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. 1.
[6] 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. 3.
[7] Lindy Muzila, Michelle Morales, Marianne Mathias and Tammar Berger, 'On the Take. Criminalizing Illicit Enrichment to Fight Corruption', The World Bank and UNODC, Washington, 2012, p. 5.

In 2010, US Attorney General Eric Holder announced the creation of a new Kleptocracy Asset Recovery Unit at the Justice Department. The unit is housed in the Asset Forfeiture and Money Laundering Section of the department's Criminal Division and is staffed by five lawyers. The Federal Bureau of Investigation's Asset Forfeiture and Money Laundering Unit, based in the bureau's Washington headquarters, has diverted two agents to assist. They supplement the work of established anti-corruption groups in US Immigration and Customs Enforcement and the FBI's Washington field office.[8]

As of early March 2014 the unit had uncovered more than US$1.1 billion in allegedly stolen funds, much of which is tied up in court.

In 2011 the anti-Kleptocracy Unit took action against Teodorin Nguema Obiang, the son of the dictator of Equatorial Guinea. The anti-corruption legal action aimed to seize a $30 million Malibu mansion, a $38 million Gulfstream Jet and over $3 million of Michael Jackson memorabilia.[9]

In March 2014 the unit seized more than $550 million of alleged proceeds of corruption related to the late Nigerian dictator Sani Abacha and his associates. Some of these funds had been channelled into major banks in New York from offshore shell companies located in the British Virgin Islands.

The work of the unit has been frustrated by the use of shell companies that are used to hide stolen money.

3. Enhancing anti-money laundering laws

Due to the privacy provision within the current anti-money laundering system within Australia it is very difficult to assess how well the system is really functioning in dealing with money laundering and terrorism financing. Where there is a lack of action it could be the result of very little criminally sourced funds entering Australia, or is it the result of a system that is not working and failing to detect or act on criminally sourced funds entering Australia? A thorough evaluation of the system would require knowledge of the actual amount of money laundering and financing of terrorism taking place, but it is only possible to know those cases that have been detected, even by those within AUSTRAC.

The recent assessment of the Centre on Law and Globalisation has raised the concern that risk-based assessment rests on the premise of evidence sufficient to weigh risk. Yet, evidence is scarce, patchy and variable on even the most basic indicators of crime, proceeds of crime, money laundering and its consequences.[10]

The Unit is deeply alarmed at the independent assessment of the effectiveness of the current global system to deal with money laundering and financing of terrorism by the Centre on Law and Globalisation, a partnership of the University of Illinois College of Law and the American Bar Foundation. They point to signs of the current global system being inadequate:[11]

[8] Andrew Marshall, 'What's Yours is Mine: New Actors and New Approaches to Asset Recovery in Global Cases', Centre for Global Development Policy Paper 018, April 2013, p. 11.
[9] Andrew Marshall, 'What's Yours is Mine: New Actors and New Approaches to Asset Recovery in Global Cases', Centre for Global Development Policy Paper 018, April 2013, p. 29.
[10] Terence C. Halliday, Michael Levi and Peter Reuter, 'Assessing the Assessors: How well do the International Monetary Fund and Financial Action Task Force evaluate national efforts to control money laundering?', Centre on Law and Globalisation, 9 January 2014, p. 22.
[11] Terence C. Halliday, Michael Levi and Peter Reuter, 'Assessing the Assessors: How well do the International Monetary Fund and Financial Action Task Force evaluate national efforts to control money laundering?', Centre on Law and Globalisation, 9 January 2014, p. 9.

- *Several of the world's most prominent international banks have been caught in flagrant and enormous repeat violations of AML/CTF regimes in countries where those regimes might have been thought to be most effective.*
- *Reports indicate that money laundering was implicated in the financial crisis in Cyprus even though AML/CTF assessments failed to signal the magnitude of a problem about illegal flows of money, which had apparently been an open secret for many years.*
- *AML/CTF assessment reports have given countries with high levels of corruption and huge flows of illicit moneys ratings on core recommendations that are similar to those of countries with low corruption and lower flows of illicit moneys.*

In their assessment "many large banks continually violate their own rules with respect to AML controls, whether intentionally or through ineffective management controls."[12] Further, "prosecuting banks or taking away their licences has been reserved for marginal players, the collateral damage of drastic action being deemed too high for major banks…."[13]

They point out:[14]

> *The FATF now explicitly acknowledges the possibilities that a country low on technical compliance might be effective and that a technically compliant country might not be effective. This de-linking of the assumed invariant positive relationship between technical compliance and outcome effectiveness potentially recognizes and can respond to the ubiquitous difficulty in global governance and regulation, namely, of countries that comply symbolically (i.e., technically) with global standards but fail to achieve the outcome objectives in global norms.*

As a result of these concerns the Unit believes that Australia needs to conduct a thorough assessment of how well its AML/CTF regime is working in reality to stem money laundering and financing of terrorism. This submission raises concerns based on cases where the Australian AML/CTF regime appears not to have worked as it should, turning away high risk or illicit flows of finance and detecting and acting on illicit financial flows. The Unit is concerned these public cases may only be the tip of the ice berg, with far more cases going undetected.

AUSTRAC and the Australian Institute of Criminology should carry out more investigation into reporting entities compliance with the AML/CTF legislation and the results of the investigation should be made public so that the Australian community can have a better idea of how well the system is functioning, similar to work that has already been carried out by the UK Financial Service Authority.[15]

The 2011 investigation by the UK Financial Services Authority into the management of high money laundering risk situations by 27 UK based banks found:[16]

---

[12] Terence C. Halliday, Michael Levi and Peter Reuter, 'Assessing the Assessors: How well do the International Monetary Fund and Financial Action Task Force evaluate national efforts to control money laundering?', Centre on Law and Globalisation, 9 January 2014, p. 54.
[13] Terence C. Halliday, Michael Levi and Peter Reuter, 'Assessing the Assessors: How well do the International Monetary Fund and Financial Action Task Force evaluate national efforts to control money laundering?', Centre on Law and Globalisation, 9 January 2014, p. 54.
[14] Terence C. Halliday, Michael Levi and Peter Reuter, 'Assessing the Assessors: How well do the International Monetary Fund and Financial Action Task Force evaluate national efforts to control money laundering?', Centre on Law and Globalisation, 9 January 2014, p. 16.
[15] Financial Service Authority, 'Bank's management of high money-laundering risk situations', June 2011.
[16] Financial Servics Authority, 'Banks' management of high money-laundering risks situations', June 2011, pp. 4-5.

Some banks appeared unwilling to turn away, or exit, very profitable business relationships when there appeared to be an unacceptable risk of handling the proceeds of crime. Around a third of banks, including the private banking arms of some major banking groups, appeared willing to accept very high levels of money-laundering risk if the immediate reputational and regulatory risk was acceptable.

Over half of the banks we visited failed to apply meaningful enhanced due diligence (EDD) measures in higher risk situations and therefore failed to identify or record adverse information about the customer or the customer's beneficial owner. Around a third of them dismissed serious allegations about their customers without adequate review.

More than a third of banks visited failed to put in place effective measures to identify customers as PEPs. Some banks exclusively relied on commercial PEPs databases, even when there were doubts about their effectiveness or coverage. Some small banks unrealistically claimed their relationship managers (RMs) or overseas offices knew all PEPs in the countries they dealt with. And, in some cases, banks failed to identify customers as PEPs even when it was obvious from the information they held that individuals were holding or had held senior public positions.

Three quarters of the banks in our sample failed to take adequate measures to establish the legitimacy of the source of wealth and source of funds to be used in the business relationship. This was of concern in particular where the bank was aware of significant adverse information about the customer's or beneficial owner's integrity.

Some banks' AML risk assessment frameworks were not robust. For example, we found evidence of risk matrices allocating inappropriate low-risk scores to high-risk jurisdictions where the bank maintained significant business relationships. This could have led to them not having to apply EDD and monitoring measures.

Some banks had inadequate safeguards in place to mitigate PMs' conflict of interest. At more than a quarter of the banks visited, RMs appeared to be too close to the customer to take an objective view of the business relationship and many were primarily rewarded on the basis of profit and new business, regardless of their AML performance.

Nearly half the banks in our sample failed to review high-risk or PEP relationships regularly. Relevant review forms often contained recycled information year after year, indicating that these banks may not have been taking their obligations to conduct enhanced monitoring of PEP relationships seriously enough.

Some banks did not carry out due diligence on their parent banks or banks in the same group, even when they were located in a higher risk jurisdiction or there were other factors which increased the risk of money laundering.

Alarmingly the FSA concluded:[17]

Despite changes in the legal and regulatory framework a number of the weaknesses identified during this review are the same as, or similar to, those identified as in the FSA report of March 2001 covering how banks in the UK handled the accounts linked to the former Nigerian military leader, General Sani Abacha….

[17] Financial Servics Authority, 'Banks' management of high money-laundering risks situations', June 2011, p. 6.

> *Serious weaknesses identified in banks' systems and controls, as well as indications that some banks are willing to enter into very high-risk business relationships without adequate controls when there are potentially large profits to be made, means that it is likely that some banks are handling the proceeds of corruption or other financial crime.*

This finding suggests it is very important that an AML/CTF regime has sufficient incentives and sanctions to drive a culture of seeking compliance with the intent of the regime, and not simply a minimalist compliance of what the reporting entity can get away with.

Given the similarities between the UK AML/CTF regime in 2011 and the Australian AML/CTF regime, it is reasonable to be concerned that similar findings might be possible amongst reporting entities in Australia. This should be tested by conducting such a study and then adjusting the AML/CTF regime if necessary based on the findings within the Australian context.

The Unit supports the current objects of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* outlined in Section 3 of the Act, with the exception in the objects of "to affect beneficially Australia's relations with foreign countries". There may be times when combating money laundering and financing of terrorism will impact negatively on Australia's relationship with specific other countries. This could arise because certain transactions by foreign politically exposed persons (PEPs) are denied for reasons of a high risk they may be transactions related to money laundering. Just because taking effective action to combat money laundering and financing of terrorism may impact negatively on Australia's relationship with other country should not be a reason in the Act for Australia not to take the effective action.

The Unit supports the following to be added to the objects of the AML/CTF Act:

- To detect and deter money laundering and financing of terrorism and reduce the risk to the integrity of the financial system.
- To provide officials with information necessary to investigate and prosecute money laundering and financing of terrorism, thereby reducing crime; and
- To provide Australia's financial intelligence unit and AML/CTF regulator with powers to collect information, supervise reporting entities and enforce AML/CTF regulations.

3.1 Need for a more 'hands-on' approach to anti-money laundering

The Unit is concerned that a greater hands-on approach is needed from regulatory authorities to ensure reporting entities take their AML/CTF obligations seriously. While many reporting entities will seek to seriously ensure they have in place an appropriate AML/CTF regime, others may seek to minimise the costs to their business by trying to get away with doing as little as possible unless required to do more by a regulatory authority. The World Bank noted on its visits to banks "revealed that the factors driving compliance with PEPs standards were reputational risk, and, to a lesser degree, regulatory risk of enforcement action."[18] The latter point is suggestive that governments need to ensure there are sufficient risk factors of sanctions for reporting entities to gain compliance with AML/CTF requirements. The view of the World Bank is that the demonstration of political will by a jurisdiction is vital in the effectiveness of anti-money laundering efforts, stating in the absence of "such political commitment, some banks will not be motivated to make a meaningful commitment to

[18] Theodore Greenberg, Larissa Gray, Delphine Schantz, Michael Latham and Carolin Gardner, 'Stolen Asset Recovery. Politically Exposed Persons. A policy paper on strengthening preventative measures', The World Bank, 2009, p. 71.

improving customer due diligence procedures with a view to detecting the proceeds of corruption."[19]

Further, even where a reporting entity under the Act is willing to take effective action against AML/CTF risks they may lack the knowledge of the typologies used by offenders relevant to their business. There is every chance that reporting entities may not be in the best position to assess the risks they face in being used for money laundering and financing of terrorism. Regulatory authorities have a vital role in ensuring that reporting entities are aware, from the significant experience of law enforcement, of the risks their business may face from money laundering and financing of terrorism.

Take for example the case of Paul Paraka the principle lawyer of Paul Paraka Lawyers. In October 2013, Mr Paraka was charged in PNG with 18 counts of allegedly receiving fraudulent payments of $28.7 million.[20] It is alleged that the law firm Paul Paraka Lawyers received these unapproved funds from PNG's Department of Finance.[21] Mr Paraka is facing 18 charges, which include: [22]

- Five counts of conspiracy to defraud the state;
- Nine counts of stealing by false pretence;
- Two counts of money laundering; and
- Two counts of dishonest application of the monies.

The case is being investigated by Fraud and Anti-Corruption Directorate detectives attached to Taskforce Sweep.[23]

Paul Paraka was a customer of NAB, and he had been transferring large sums of money to contacts in Australia (in the Gold Coast and NSW).[24] Investigations by journalists found bank accounts linked to Mr Paraka have transferred nearly $3 million into Australia, including a three-part $80,000 transaction to his Australian-based wives and girlfriends, including one that was living in the Star City Casino complex.[25] It has been alleged that PNG investigators believe that most of the funds were corruptly obtained.[26]

In response to a *Today Tonight* program raising the allegations with regards to Mr Paraka, NAB issued the following statement:[27]

> *National Australia Bank takes all allegations of money laundering seriously. Payments NAB deems as suspicious will be blocked and reported, as required by law.*
>
> *In late 2012, NAB launched a thorough investigation regarding some funds transfers from Papua New Guinea, based on information provided by the Australian Federal Police and other law enforcement agencies in both Australia and PNG.*

---

[19] Theodore Greenberg, Larissa Gray, Delphine Schantz, Michael Latham and Carolin Gardner, 'Stolen Asset Recovery. Politically Exposed Persons. A policy paper on strengthening preventative measures', The World Bank, 2009, p. xv.
[20] ABC Australia, 'Papua New Guinea Lawyer Paul Paraka charged over $30 million in fraudulent payments', 24 October, 2013; and Rowan Callick, 'Top PNG lawyer arrested over $28m', *The Australian*, 25 October 2013.
[21] ABC Australia, 'PNG's PM threatens Finance Department', 22 May, 2013.
[22] ABC Australia, 'Papua New Guinea Lawyer Paul Paraka charged over $30 million in fraudulent payments', 24 October, 2013.
[23] 'Cops get boot', *Post Courier,* 13 January 2014.
[24] Nick McKenzie and Richard Baker, 'PNG dirty money trail leads to Australia', *The Age*, July 19, 2013.
[25] Ibid.
[26] Ibid.
[27] Today Tonight, 'PNG money laundering', 26 August 2013, http://au.news.yahoo.com/today-tonight/lifestyle/article/-/18659424/png-money-laundering/ (accessed 14 September 2013)

> *Following NAB's investigation, some customers' accounts were closed and some payments originating from PNG were declined.*

So from the public statement by NAB on the matter it would appear the bank was, at best, unaware of the risks it was taking in dealing with politically exposed persons from PNG, until the matter was brought to their attention by Australian and PNG law enforcement authorities. By its own admission the bank was not the entity best placed to understand the risks it was entering into and could not be relied upon to take the necessary action without the guidance of law enforcement authorities.

There were serious findings against Mr Paraka by the PNG Government Commission of Inquiry generally into the Department of Finance in their report completed at the end of October 2009. While court action suppressed publication of the Commission of Inquiry final report in PNG, the document was readily accessible on the internet. However, the NAB, by their own statement, did not take appropriate action until the matter was raised with them by law enforcement authorities in 2012.

In addition, the US prosecution of Liberty Reserve may also point to inadequacies in Australia's AML regime, as three Westpac bank accounts are amongst the 45 bank accounts the US obtained seizure warrants or restraining orders on.[28] US authorities sought to seize the assets in three Westpac accounts held by Technocash Ltd holding up to $36.9 million.[29] Technocash Limited was an Australian registered company. The funds are alleged to be connected to shell companies owned by the defendants in the case.[30] 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 customers 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:[31]

> *…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*

[28] US Attorney for the Southern District of New York, 13 Civ 3565, 28 May 2013, p. 10; and USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 43.
[29] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 29, 43.
[30] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 21.
[31] US Attorney for the Southern District of New York, 13 Civ 3565, 28 May 2013, pp. 4-5.

Reserve processed an estimated 55 million separate financial transactions and is believed to have laundered more than $6 billion in criminal proceeds.

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.[32]

US authorities alleged defendant Arthur Budovsky used Technocash to receive funds from exchangers. Mr Budovsky, the alleged principal founder of Liberty Reserve,[33] allegedly used his bank to wire funds to Technocash bank accounts held by Westpac.[34] 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 anmd November 2012 of more than $300,000.[35]

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.[36] 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.[37] 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.[38]

It is alleged Arthur Budovsky was the president of Grupo Lulu Limitada which was allegedly used to transfer and disguise Liberty Reserve Funds.[39] 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.[40]

Further, defendant Azzeddine El Amine, manager of Liberty Reserve's financial accounts,[41] 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 El Amine, notifying him of the transfer. Based on these alerts, it is alleged between 12 June

[32] US Attorney for the Southern District of New York, 13 Civ 3565, 28 May 2013, p. 6.
[33] 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.
[34] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 29.
[35] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 36.
[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 Money Laundering Scheme', 28 May 2013.
[37] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 37.
[38] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 36.
[38] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 38.
[39] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 36.
[39] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 40.
[40] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 36.
[40] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 41.
[41] 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.

2012 and 1 May 2013, exchangers doing business with Liberty Reserve send approximately $36,919,884 to accounts held by Technocash at Westpac.[42]

The defendants are alleged to have used Technocash services to transfer funds to nine Liberty Reserve controlled accounts in Cyprus.[43]

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.[44] 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."[45]

The Justice and International Mission Unit notes that in 2009, the Australian Institute of Criminology (AIC) conducted a survey of 4,346 Australian businesses with anti-money laundering and counter-terrorism financing (AML/CTF) obligations under Australian legislation. The Unit is concerned about the level of complacency this revealed amongst some reporting entities. For example, respondents from the cash delivery service sector were most likely to believe that there would be no money laundering risk for their businesses in the two years to 30 June 2011 (43.9%), while a further 21.1 percent anticipated that such risk would be low or would decrease.[46] Approximately 11 percent of respondents stated that there were low risks, or no risks associated with money laundering and that, accordingly, they did not see the need for any countermeasures. The extent to which respondents stated that there were no risks of money laundering to their businesses and accordingly, no anti-money laundering measures were needed, varied significantly according to the respondent's business sector. Cash delivery services was the sector most likely to indicate that no risks were present and that no measures were necessary to address money laundering (19.3%). In the banking sector 10.2% of respondents believed there was no need for money laundering counter measures. Only 4.7 percent of respondents from the alternative remittance sector considered there to be no risks and no countermeasures required.[47]

The AIC found that 20% of businesses they surveyed were not compliant with AML know-your-customer requirements. Businesses from the financial services sector were significantly more likely than other businesses to perform ongoing due diligence and know your customer procedures.[48] However, even here 7.3% of financial services businesses did not conduct on-going due diligence for existing customers, and this increased to 9.9% for banks and 15.8% for foreign exchange businesses.[49]

[42] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 30.
[43] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 31.
[44] Technocash, 'Opportunity: Own the Technocash Payment Platform', Media Release, 5 July 2013.
[45] http://www.technocash.com/pages/press-release.cfm
[46] Julie Walters, Russell Smith, Brent Davis, Kim-Kwang Raymond Choo and Hannah Chadwick, "The anti-money laundering and counter-terrorism financing regime in Australia: Perceptions of regulated businesses in Australia", Australian Institute of Criminology Report 117, 2012, p. 15.
[47] Julie Walters, Russell Smith, Brent Davis, Kim-Kwang Raymond Choo and Hannah Chadwick, "The anti-money laundering and counter-terrorism financing regime in Australia: Perceptions of regulated businesses in Australia", Australian Institute of Criminology Report 117, 2012, p. 21.
[48] Julie Walters, Russell Smith, Brent Davis, Kim-Kwang Raymond Choo and Hannah Chadwick, "The anti-money laundering and counter-terrorism financing regime in Australia: Perceptions of regulated businesses in Australia", Australian Institute of Criminology Report 117, 2012, p. xiv.
[49] Julie Walters, Russell Smith, Brent Davis, Kim-Kwang Raymond Choo and Hannah Chadwick, "The anti-money laundering and counter-terrorism financing regime in Australia: Perceptions of regulated businesses in Australia", Australian Institute of Criminology Report 117, 2012, pp. 27-28.

The AIC survey of businesses with regards to AML/CTF compliance also found 21.4% of respondents were not confident about know your customer procedures identifying foreign owned companies.[50]

The findings suggest that reporting entities cannot be relied on universally to make realistic assessments of money laundering and terrorism financing risks without guidance from law enforcement bodies.

Similar findings were made by UK Financial Services Authority in their 2012 assessment of UK investment banks compliance with anti-bribery and anti-corruption requirements. They quote one case in which:[51]

> *A senior individual at one large firm who had been interviewed as part of the firm's risk assessment process told us there was no bribery and corruption risk in his business unit. However, he then described what we considered higher risk business practices, including frequent interaction with public officials in higher risk countries, gifts to public officials to foster good relations, and his ability to influence the recruitment process in the firm.*

In another example:[52]

> *One small firm had not completed a formal risk assessment, believing it to be unnecessary due to the firm's small size. Instead, the firm stated that its senior management had discussed and identified bribery and corruption risks across the business and also countries that were considered to be corrupt or involved in tax evasion.*

3.2 Greater focus on Politically Exposed Persons

For field work conducted on banks globally, the World Bank expressed concern that:[53]

> *Although the banks visited as part of the field work were well-versed in applying a risk-based approach, it was suggested that some banks were abusing its flexibility (for example, tailoring it to suit their business model rather than their risk model). These banks use the risk-based approach to apply PEP measures in a manner that does not account for all the risks, or resort to box-checking approach.*

Only a minority of businesses surveyed by the Australian Institute of Criminology regarded politically exposed persons (PEPs) as high-risk customers with regards to money-laundering. Only 38.2% of banks and 15.2% of gambling providers regarded PEPs as high risk customers.[54] Collectively, only 22% of the reporting entities surveyed believed PEPs were high risk customers for money laundering.[55] Further only 51.2% of respondent businesses

[50] Julie Walters, Russell Smith, Brent Davis, Kim-Kwang Raymond Choo and Hannah Chadwick, "The anti-money laundering and counter-terrorism financing regime in Australia: Perceptions of regulated businesses in Australia", Australian Institute of Criminology Report 117, 2012, p. 31.
[51] Financial Services Authority, 'Anti-bribery and corruption systems and controls in investment banks', March 2012, p. 16.
[52] Financial Services Authority, 'Anti-bribery and corruption systems and controls in investment banks', March 2012, p. 18.
[53] Theodore Greenberg, Larissa Gray, Delphine Schantz, Michael Latham and Carolin Gardner, 'Stolen Asset Recovery. Politically Exposed Persons. A policy paper on strengthening preventative measures', The World Bank, 2009, p. 23.
[54] Julie Walters, Russell Smith, Brent Davis, Kim-Kwang Raymond Choo and Hannah Chadwick, "The anti-money laundering and counter-terrorism financing regime in Australia: Perceptions of regulated businesses in Australia", Australian Institute of Criminology Report 117, 2012, p. 13.
[55] Julie Walters, Russell Smith, Brent Davis, Kim-Kwang Raymond Choo and Hannah Chadwick, "The anti-money laundering and counter-terrorism financing regime in Australia: Perceptions of regulated businesses in Australia", Australian Institute of Criminology Report 117, 2012, p. 15.

were confident that they would identify transactions involving PEPs.[56] This is suggestive the AML/CTF regime needs to be enhanced to ensure reporting entities treat PEPs with a greater amount of seriousness when it comes to money laundering risks. The Unit notes that AUSTRAC has recently increased requirements of reporting entities around PEPs, but it is yet to be seen if these changes result in reporting entities treating the money laundering risks associated with PEPs more seriously and if it results in greater detection and action in relation to money laundering cases involving PEPs. The Unit would encourage a thorough evaluation of the impact of these new rules after an appropriate time has been allowed for their implementation.

The Unit would prefer to see great prescription on reporting entities when dealing with PEPs. The Unit urges that the Australian Government implement the following recommendations of the World Bank that:[57]

> *A public official should be asked to provide a copy of any asset and income declaration form filed with their authorities, as well as subsequent updates. If a customer refuses, the bank should assess the reasons and determine, using a risk-based approach, whether to proceed with the business relationship. More than 110 countries require that their public officials file asset and income disclosure forms. Although only one bank was found that asks customers for a copy of the form, all banks agreed that it was an additional tool and noted that they ask for the same information and more during account opening….*

Also:

> *Where a person has ceased to be entrusted with a prominent public function, countries should not introduce time limits on the length of time the person, family member, or close associate needs to be treated as a PEP.*

The World Bank and the UNODC publicly called for disclosure of public officials' income, assets and interests to be mandated in March 2012.[58]

Further, banks and other financial institutions should be required to disclose full details of foreign state assets that they manage. In dictatorships where one individual, or a small cabal, exercises almost complete power over the state, there is a very thin dividing line between state and personal investments. For example, it appears that Muammar al-Gaddafi had significant personal control over the state funds invested in the Libyan Investment Authority, which Global Witness revealed were managed by major international banks.

The Unit is further deeply concerned that the AIC survey of businesses in 2009 found less than one-quarter of businesses indicated that they used software for AML/CTF compliance purposes. Those in the gambling sector were the least likely to use AML/CTF software.[59] It is difficult to see how a business would be able to have any reasonable chance to detect PEPs without the use of some software database of PEPs, especially in relation to relatives and close associates of political figures and foreign officials. However, a challenge noted by the World Bank is that some of the commercial PEP databases will generate a lot of false

[56] Julie Walters, Russell Smith, Brent Davis, Kim-Kwang Raymond Choo and Hannah Chadwick, "The anti-money laundering and counter-terrorism financing regime in Australia: Perceptions of regulated businesses in Australia", Australian Institute of Criminology Report 117, 2012, p. 40.
[57] Theodore Greenberg, Larissa Gray, Delphine Schantz, Michael Latham and Carolin Gardner, 'Stolen Asset Recovery. Politically Exposed Persons. A policy paper on strengthening preventative measures', The World Bank, 2009, p. xvii.
[58] The World Bank and UNODC, 'Disclosure of Assets and Income by Public Officials is Crucial to Curbing Corruption, Finds New StAR Study', Media Release, 28 March 2012.
[59] Julie Walters, Russell Smith, Brent Davis, Kim-Kwang Raymond Choo and Hannah Chadwick, "The anti-money laundering and counter-terrorism financing regime in Australia: Perceptions of regulated businesses in Australia", Australian Institute of Criminology Report 117, 2012, p. xiv.

positives (people with the same name as the customer or beneficial, but who are not the customer or beneficial owner).[60]

The World Bank has noted that, as examples of good practice, some banks globally run their customer list against commercial or in-house PEP databases on a regular basis, often daily or weekly. This practice ensures that the bank captures those customers who attain PEP status after the customer take-on process. Once these customers are identified, they are then reviewed by senior management, placed on the PEP customer list, and enhanced due diligence is applied.[61]

The World Bank has also noted that many banks they spoke to include a PEP check when a customer requests an additional product or specific service. This routine is particularly important if the risk of money laundering associated with the new product is considered to be higher than with existing products the customer holds. In their view, PEP checks should form part of this risk consideration.[62]

The World Bank has recommended that PEP customers should be reviewed by senior management or a committee including at least one senior manager using a risk-based approach, at least yearly, and the results of this review should be documented. Further, they recommend PEP customers should be reviewed annually by an audit committee, board or equivalent corporate governance body as part of its risk-management responsibilities.[63]

The World Bank noted that in order to motivate staff to take enhanced due diligence of PEPs more seriously a bank produced a short video presentation on "Why monitor PEPs?", which provided an overview of the destructive effects of corruption around the world.[64]

3.3 Terminating suspicious business relationships

Sam Koim, head of the PNG anti-corruption body Task Force Sweep stated that where it was not possible to conduct a "means test" on a person from PNG transferring funds to Australia, so that the recipient knows how the money was generated, "we ask that you refuse to perform the transaction and that you terminate the business relationship".[65] The Unit supports this request more broadly to require business entities not to do business with people who are high money laundering risks, unless the reporting entity is satisfied the funds have a legitimate source. The exception to this is where Australian law enforcement authorities intend to mount an investigation with the view to a prosecution or assisting in a prosecution and not conducting the business would jeopardise the possible prosecution. As this is an extremely rare occurrence with regards to foreign PEPs, there will be many circumstances where it is simply better for the reporting entity to not enter into a business

[60] Theodore Greenberg, Larissa Gray, Delphine Schantz, Michael Latham and Carolin Gardner, 'Stolen Asset Recovery. Politically Exposed Persons. A policy paper on strengthening preventative measures', The World Bank, 2009, p. 45.
[61] Theodore Greenberg, Larissa Gray, Delphine Schantz, Michael Latham and Carolin Gardner, 'Stolen Asset Recovery. Politically Exposed Persons. A policy paper on strengthening preventative measures', The World Bank, 2009, p. 34.
[62] Theodore Greenberg, Larissa Gray, Delphine Schantz, Michael Latham and Carolin Gardner, 'Stolen Asset Recovery. Politically Exposed Persons. A policy paper on strengthening preventative measures', The World Bank, 2009, p. 34.
[63] Theodore Greenberg, Larissa Gray, Delphine Schantz, Michael Latham and Carolin Gardner, 'Stolen Asset Recovery. Politically Exposed Persons. A policy paper on strengthening preventative measures', The World Bank, 2009, p. 55.
[64] Theodore Greenberg, Larissa Gray, Delphine Schantz, Michael Latham and Carolin Gardner, 'Stolen Asset Recovery. Politically Exposed Persons. A policy paper on strengthening preventative measures', The World Bank, 2009, p. 72.
[65] Sam Koim, AUSTRAC Major Reporters Meeting, Sydney, 4 October 2012, p.5.

relationship with a high risk person where the legitimate source of the funds cannot be established.

The AML/CTF regime should be modified to allow financial institutions to terminate customer relationships where they believe there is a high risk that funds deposited with them have an illicit source. Currently, financial institutions face the possibility of prosecution if they do anything to disclose to a customer they have notified Australian authorities that the financial institution has a suspicion the funds in question may violate Australia's anti-money laundering laws. This risk of prosecution may contribute to financial institutions failing to end relationships with customers where they suspect the customer is engaged in money laundering activities. The anti-money laundering law should allow a reporting entity, to terminate a relationship with a customer if, after having submitted a suspicious transaction report to AUSTRAC, it has not received any response from AUSTRAC or other authorised office of an authorised agency within seven days. This will help to place pressure on Australian authorities to act in a timely manner on suspicious transaction reports. In the UK, the *Proceeds of Crime Act 2002* makes it a money-laundering offence to handle criminally obtained funds, unless an authorised disclosure is made and consent to handle the funds is obtained from the National Crime Authority.[66] The National Crime Authority has seven working days to grant or deny consent to handle the criminally obtained funds.

If the financial institution, or other reporting entity, continues to deal with funds from a customer where they have strong concerns the customer is engaged in money laundering, then they should face the risk of prosecution for doing so. This will force financial institutions and other reporting entities to take action where they hold strong suspicions around a customer.

As an example of PNG government funds having been allegedly transferred from Papua New Guinea to Australia without following proper procedures[67] there is the case of the Motor Vehicle Insurance Limited transfer to Woodlawn Capital Pty Ltd. In November 2011 the Minister for Public Enterprises, Sir Mekere Morauta, publicly alleged that:[68]

> *MVIL sold the shares when under the control of the former Minister for Public Enterprises, Arthur Somare, and the former IPBC [Independent Public Business Corporation] management. Proper processes had not been followed, and the sale is in breach of Section 45B of the IPBC Act and Section 110 of the Companies Act. The sale was not approved by the IPBC board, as required, and there was no shareholders' resolution approving the sale, as required.*

Approximately K96 million was invested by the Motor Vehicle Insurance Limited into Australian company Woodlawn Capital Pty Ltd. Attempts by the PNG Government to repatriate these funds have so far been unsuccessful.

The funds transferred by MVIL to Woodlawn Capital are alleged to be the proceeds of the sale of 530,105,100 shares in the Bank South Pacific which were owned by MVIL. The sale, to a company called Nominees Niugini Limited, was the subject of a PNG police investigation.[69] The IPBC commenced legal proceedings against MVIL and Nominees Niugini Limited.[70] A directions hearing was scheduled with the PNG Supreme Court of Justice and Nominees Niugini Limited against the MVIL and the Independent Public Business

[66] National Crime Agency, 'Obtaining consent from the NCA under Part 7 of the Proceeds of Crime Act (POCA) 2002 or under Part 3 of the Terrorism Act (TACT) 2000', October 2013.
[67] Transparency International PNG, 'Motor Vehicle Insurance Limited (MVIL) Scandal', http://www.transparencypng.org.pg/index.php/scandals/view/motor-vehicle-insurance-limited-mvil-scandal, 4 December 2013.
[68] Mekere Morauta, Minister for Public Enterprises, Public Statement, 23 November 2011.
[69] Mekere Morauta, Minister for Public Enterprises, Public Statement, 23 November 2011.
[70] Mekere Morauta, Minister for Public Enterprises, Public Statement, 23 November 2011.

Corporation for 5 November 2013. Of Nominee Niugini's three directors, two were Australians as of 19 August 2013.

The case raises the question of what steps were taken by any Australian bank that received the original transfer from MVIL to Australia to determine the legitimacy of the transfer and that the PNG authorities had approved the transfer.

3.4 AML requirements of foreign subsidiaries

The Unit is concerned the FATF review of Australia's compliance with the FATF standards found:

> *409. There is no legal obligation or guidance requirement under the FTR Act that, where the minimum AML/CTF requirements of the home and host countries differ, branches and subsidiaries in the host countries are required to apply the higher standard, to the extent that local (i.e. host country) laws and regulations permit. Equally, there is no requirement that financial institutions be required to inform their home country supervisor when a foreign branch or subsidiary is unable to observe appropriate AML/CTF measures because it is prohibited by local (i.e. host country) laws, regulations or other measures.*

This was confirmed as being correct by an e-mail from the Attorney General's Department in February 2010, that stated:[71]

> *There is no specific requirement for branches and subsidiaries to apply the higher AML/CTF standard where the obligations between the home and host countries differ. Neither is there an obligation on reporting entities to inform AUSTRAC when a foreign branch or subsidiary is unable to observe AML/CTF systems and procedures due to the local laws.*

The Unit therefore urges the Australian Government to fully implement the FATF recommendation that:

> *413. Australia should also adopt legal requirements for branches and subsidiaries to apply the higher AML/CTF standard, to the extent that the laws of the host country allows. In the event where a foreign branch or subsidiary is unable to observe appropriate AML/CTF measures because this is prohibited by local (i.e. host country) laws, regulations or other measures, those financial institutions should be required to inform Australian authorities. Financial institutions should also be required to pay particular attention that the principle is observed wherewith to branches and subsidiaries in countries which do not or insufficiently apply the FATF recommendations.*

3.5 Designated Non-Financial Businesses and Professions

The Unit believes there is a need to add designated non-financial businesses and professions (DNFBP) more thoroughly to the AML/CTF regime, in line with the FATF AML/CTF Recommendations. The measure is currently under consideration by the Attorney General's Department and AUSTRAC through the statutory review of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006.*

The World Bank and UN Office on Drugs and Crime (UNODC) published a report reviewing some 150 cases of corruption where the money from laundered. In the majority of cases:[72]

- A corporate vehicle was misused to hide the money trail;
- The corporate vehicle in question was a company or corporation;

[71] E-mail from Attorney-General's Department to the JIM Unit, 19 February 2010.
[72] 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.

- The proceeds and instruments of corruption consisted of funds in a bank account; and
- In cases where the ownership information was available, the corporate vehicle in question was established or managed by a professional intermediary.

In two-thirds of the cases some form of surrogate, in ownership or management, was used to increase the opacity of the arrangement.[73] In half the cases where a company was used to hide the proceeds of corruption, the company was a shell company.[74] One in seven of the companies misused were operational companies, that is 'front companies'.[75] Based on these findings it is particularly important to capture corporate service providers within the AML/CTF regime.

Further the examples of Eremas Wartoto, Paul Tiensten and Jeffery Yakopya (outlined in section 5.4 below), who all were able to buy property in Australia, outlined above may point to value in including real estate agents and lawyers within the AML/CTF regime if any of the money used in making these purchases did not have a legitimate source.

In addition, Leonard Capon is an Australian business man, who was arrested and charged by Task-Force sweep after allegedly misappropriating K1,485,085 ($668,400) through his company Rural Development Services. This money was reported to be intended for a mini-hydro power plant in PNG highlands, which never eventuated.[76]

Leonard Capon owns one property in Queensland, in Dunkeith Avenue, Benowa, bought for $835,000 in April 2009. The ANZ Bank acted as the mortgagee.

He has also bought and sold a property in Queensland, in Ferry Road, Southport, which was jointly owned with Diana Dauge Dona. It was bought for $500,000 in August 2012. It was sold for $440,000 just over six months later in February 2013.

Clearly lawyers and real estate agents would have been involved in the purchases of properties in Queensland related to each of these people and it is not known to the Unit if any of these bodies undertook due diligence to assure themselves the funds used in each transaction had a legitimate source. The Unit notes that of the people named, only Paul Tiensten has been convicted of the offences he was arrested for.

A Canadian study found that lawyers came into contact with the proceeds of crime in 49.7% of all cases examined, and that lawyers are implicated in money laundering (both wittingly and unwittingly) primarily through their role as an intermediary in a commercial or financial transaction.[77] However, the study concluded that mandatory reporting for legal professionals should only apply to financial and business transactions conducted by lawyers on behalf of their clients.

The Unit accepts there is a balance to be struck between the reporting obligations to be placed upon DNFBP and the level of suspected money laundering activity that is taking place involving these entities.

---

[73] 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.
[74] 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.
[75] 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.
[76] 'Australian man charged with fraud in PNG', *The Australian,* 25 November 2012; and Sam Koim, 'Investigation Taskforce Sweep June 2013 Report', *Post Courier,* 2 August 2013, p. 46.
[77] Maria Italia,'Lawyers and accountants as "gatekeepers" to combat money laundering – an international comparison', *AT Rev **42*** (2013), p. 138.

3.6 Need for greater co-operation with developing countries

The Unit believes there is a need to enhance international co-operation with developing countries where there is a reasonable likelihood that money stolen from governments in those countries will be laundered through Australia.

In a question to the Government from Senator Scott Ludlam, the Government indicated that Australian police only assist PNG police in corruption investigations where the PNG police make an explicit request for assistance. If Australian police were to become aware of corruptly or criminally obtained funds entering Australia, they would not automatically share that information with the PNG police.[78] This situation may have subsequently improved after the signing of an intelligence sharing agreement between the Australian Federal Police and Taskforce Sweep in December 2013.[79] However, it is our understanding that information will still only be provided to the PNG anti-corruption unit Taskforce Sweep by the AFP when Taskforce Sweep makes an explicit request for the information.

A lack of trust appears to exist from Australian authorities towards PNG authorities. The World Bank and the UNODC have identified that a lack of trust between jurisdictions does inhibit and delay the provision of mutual legal assistance. They have recommended that jurisdictions should adopt policies and procedures that cultivate trust and improve communication, such as:[80]

- Legislation allowing for the spontaneous sharing of information with another jurisdiction;
- Communication strategies whereby developed countries provide technical support and other assistance on communication issues faced by developing jurisdictions; and
- Policies encouraging participation at relevant international and bilateral meetings and in particular networks, including regional asset recovery networks.

AUSTRAC will generally only share information with overseas FIUs where a formal exchange agreement exists. At the moment there are 68 such agreements in place. To its credit AUSTRAC does exchange information with some developing and middle income countries, including Argentina, Brazil, Chile, Colombia, Fiji, Guatemala, India, Indonesia, Malaysia, Mexico, the Philippines, South Africa, Sri Lanka, Thailand and Venezuela.[81]

Australia should automatically share information with authorities of other governments (especially foreign FIUs) when a foreign PEP purchases property in Australia, transfers funds to an Australian bank account or gambles at an Australian casino or other gambling venue, unless the Australian authorities have some reason to carry out a prosecution of the person in question themselves or entities involved in the transaction and the sharing of information would compromise that prosecution. Further, such information should not be shared if the Australian Government has reasonable concerns the information is likely to be used to carry out human rights abuses against the PEP in question. As in the vast majority of cases, Australian authorities would not carry out any investigation or legal action themselves against a foreign PEP in relation to suspicious transactions it is hard to see that anything is lost by automatically sharing the information above with authorities of other governments. Information about property purchases is publicly available anyway, at a small cost. However, being alerted in a timely manner of such transfers may assist developing country authorities

[78] Senator Scott Ludlam, Senate Question Number 2391, 19 October 2012.
[79] 'Police aid for PNG', *The Herald Sun,* 6 December 2013.
[80] 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. 6.
[81] The Auditor-General, "AUSTRAC's Administration of its Financial Intelligence Function", Australian National Audit Office, Audit Report No 47 2012-23, June 2013, pp. 69, 107; and AUSTRAC Annual Report 2012-13, 10 October 2013, p. 8.

in any investigations they are undertaking or may alert them to the need for an investigation. In fact the World Bank and UNODC have further recommended:[82]

> *When a suspicious transaction report (STR) is linked to a foreign PEP, the competent authorities should, after proper analysis supports such dissemination, share this information with the competent authorities in the PEP's home jurisdiction and any other germane jurisdiction.*

3.7 Requirements around disclosure of beneficial ownership

While AUSTRAC has introduced new rules around beneficial ownership and enhanced due diligence, more could be done. For example, the AIC conducted interviews with employees from reporting entities and found opaque transactions identified by an interviewee in the mutual banking industry encompassed internet banking services, where the business has a decreasing amount of contact with customers, and in the capacity for account holders to nominate third-party signatories or power of attorney access to accounts. This left the business unsure about who was transacting through the account.[83]

As an example of an improvement that could be made around disclosure of beneficial ownership, the World Bank has pointed out that in one jurisdiction, that they did not name, the customer is required to complete a written declaration of the identity and details of the beneficial owner(s) – a requirement pursuant to an agreement between the jurisdiction's bankers association and signatory banks. The form is signed and dated by the contracting party and includes a statement that it is a criminal offence (document forgery) to provide false information on the form, with a penalty of up to five years or a fine. The form approach has been adopted by banks in other jurisdictions, even when not required by law or regulation. In the jurisdiction where the form is used, the prosecuting authority has prosecuted cases of forgery (that is, falsely establishing in a written document a fact with legal application or what is referred to as an 'intellectual lie').[84]

The World Bank argues the written declaration of beneficial ownership is a valuable tool for a number of reasons. It assists in focusing on the process of identification of the beneficial owner at the outset, not only for the bank officials but also for the contracting party. It provides the background information that will assist the bank with verification, as well as in determining if the beneficial owner(s) is a PEP. It assists regulatory authorities in evaluating beneficial ownership practices and enables better oversight of how banks are handling beneficial ownership issues. Finally, the requirement to sign under penalty of a criminal offence and, where appropriate, the additional consequences of non-conviction based or criminal forfeiture, serves to alert the contracting party to the seriousness and importance of the information and therefore acts as a deterrent. It may not be a deterrent for the corrupt PEP, but for intermediaries and others (including family and close associates) who are acting as the contracting party.[85]

---

[82] 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. 36.
[83] Julie Walters, Russell Smith, Brent Davis, Kim-Kwang Raymond Choo and Hannah Chadwick, "The anti-money laundering and counter-terrorism financing regime in Australia: Perceptions of regulated businesses in Australia", Australian Institute of Criminology Report 117, 2012, p. 18.
[84] Theodore Greenberg, Larissa Gray, Delphine Schantz, Michael Latham and Carolin Gardner, 'Stolen Asset Recovery. Politically Exposed Persons. A policy paper on strengthening preventative measures', The World Bank, 2009, p. 37.
[85] Theodore Greenberg, Larissa Gray, Delphine Schantz, Michael Latham and Carolin Gardner, 'Stolen Asset Recovery. Politically Exposed Persons. A policy paper on strengthening preventative measures', The World Bank, 2009, p. 37.

4. Registry of Company and Trust Ownership

The Unit strongly urges that the Australian Government follow the example of the UK Government and introduce a public registry of who ultimately owns and controls Australian companies. The public registry was announced on 21 April 2014.[86] The UK Government has stated on announcing the public registry "It is hoped greater transparency will mean honest entrepreneurs and investors can do business more securely in the UK and not be disadvantaged by those who do not play by the rules."

Shell companies in which the ultimate beneficial ownership is concealed are commonly used in financially related serious crimes, as demonstrated by the Liberty Reserve case above demonstrates. The World Bank and UN Office on Drugs and Crime (UNODC) published a report reviewing some 150 cases of corruption where the money from laundered. In the majority of cases:[87]

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

In two-thirds of the cases some form of surrogate, in ownership or management, was used to increase the opacity of the arrangement.[88] In half the cases where a company was used to hide the proceeds of corruption, the company was a shell company.[89] One in seven of the companies misused were operational companies, that is 'front companies'.[90]

The UK Government public registry of company ownership includes:[91]

- A central open registry of information on companies' ultimate controllers and owners maintained by Companies House. The registry would hold information on individuals with an interest in more than 25% of shares or voting rights in a company, or who otherwise control the way a company is run. Companies will need to supply these details to Companies House when starting up and update them at least once every 12 months. This will include details such as name, date of birth and nationality.
- Making sure that front directors, who often hold multiple directorships, are aware of their statutory duties when they start. The UK Government revealed that 6,150 people currently act as directors of more than 20 UK registered companies, with some people being directors in over 1,000 companies.

Earlier research by World-Check found 3,994 exact matches of high risk individuals found to be registered directors of companies in the UK.[92] World-Check found 1,504 disqualified directors running current UK companies despite the existence of the Register of Disqualified Directors. Many of these Disqualified Directors are currently operating companies from prison. The screening also revealed 154 individuals involved in financial crime, 13 individuals

[86] The Rt Hon DR Vince Cable MP, 'Tough action promised on hidden company owners', www.gov.uk, 21 April 2014.
[87] 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.
[88] 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.
[89] 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.
[90] 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.
[91] The Rt Hon DR Vince Cable MP, 'Tough action promised on hidden company owners', www.gov.uk, 21 April 2014.
[92] http://www.prnewswire.co.uk/news-releases/world-check-exposes-terrorists-financial-criminals-and-disqualified-directors-in-uk-companies-house-register-152571225.html

who are either wanted by Interpol for terrorism or associated with terrorist groups and activities, 37 narcotics traffickers, nearly 1000 domestic and foreign Politically Exposed Persons and hundreds of individuals from many other high risk categories.

An individual, wanted by Interpol for terrorism and forgery, was listed in the register as Director of 12 UK companies. Two individuals, both suspects in foiled UK terror plots, were listed by Companies House to be Directors of several UK companies. An Eastern European General who was facing United Nations war crimes charges was registered as the Director of one active UK registered company.

We have no way of knowing if similar results would occur in Australia and are unaware of any reporting by government authorities that indicates this would not be the case.

The UK announcement on a public registry of beneficial ownership of companies followed a G8 promise in June 2013 that the G8 countries would each produced a beneficial ownership action plan.[93] France has indicated that it plans to follow the UK example with a public registry of beneficial ownership.

In 2011, the World Bank and the UNODC had recommended that details of company directors should be made "publicly available in all company registries. In cases in which the director is acting as a nominee for another person, that fact should be noted in the registry, along with the name of that "shadow director"."[94] They argued such public registries should hold information on owners, shareholders and members of legal entities "which should cover anyone whose ownership stake is sufficiently large to be deemed a controlling interest."[95] Further:[96]

> *In addition to improving the data content in company registries, countries should strive to make it freely available. Ideally, this would mean providing free online access (without preregistration requirements or subscription fees), complete with search functions that allow for extensive cross-referencing of the data. Access to historical records on the legal entities entered in the register also should be included.*

5. Dealing with unexplained wealth

Legislation to deal with unexplained wealth is one of the tools needed to deal with funds stolen from developing countries and shifted into Australia. We welcome the current legislation before the Parliament, the *Crimes Legislation Amendment (Unexplained Wealth and Other Measures) Bill* 2014, that goes part way towards implementing the previous 2012 recommendations of the Joint Committee on Law Enforcement's recommendations out of the inquiry into Commonwealth unexplained wealth legislation and arrangements. We support the position of the Police Federal of Australia and the Australian Federal Police Association on the need for a pure unexplained wealth regime without a predicate offence to be able to target assets at the layering and integration stages of a money laundering operation.[97] We note the experience of these bodies that the inclusion of the requirement for a predicate

[93] Global Witness and Christian Aid, 'Company Ownership: which places are the most and least transparent', November 2013, p. 2.
[94] 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. 4.
[95] 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. 4.
[96] 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. 5.
[97] Police Federation of Australia and the Australian Federal Police Association, Submission to the Senate Committee on Legal and Constitutional Affairs on *Crimes Legislation (Organised Crime and Other Measures) Bill,* 31 January 2013, p. 6.

offence meant the unexplained wealth provisions had never been used in practice.[98] At the same time we understand that constitutional requirements limit Commonwealth unexplained wealth provisions.[99] We support recommendation 15 of the previous Parliamentary Joint Committee on Law Enforcement inquiry into unexplained wealth legislation that supported a "national unexplained wealth scheme, where unexplained wealth provisions are not limited by having to prove a predicate offence."[100]

5.1 International Standards and Laws in Other Jurisdictions

By 2010, over 40 jurisdictions has introduced legislation criminalising illicit enrichment.[101] Illicit enrichment was introduced as a mandatory offence in the 1996 Inter-American Convention against Corruption. The *UN Convention Against Corruption*, to which Australia is a state party, adopted a position in Article 20 that states should consider criminalising illicit enrichment by public officials "subject to the requirements of their constitutions and the fundamental principles" of their legal systems.[102] Article 12(7) of the UN *Convention on Transnational Organised Crime*, to which Australia is a states party, states that jurisdictions "may consider the possibility of requiring an offender demonstrate the lawful origin of alleged proceeds of crime or other property liable to confiscation, to the extent that such a requirement is consistent with the principles of their domestic law and with the nature of the judicial and other proceedings."

The World Bank and the UNODC point out that properly constructed legislation for the restraint and confiscation of unexplained wealth is consistent with human rights standards. The jurisprudence of the European Court of Human Rights clearly delineates that the presumption of innocence does not prevent legislatures from creating criminal offenses containing a presumption by law as long as the principles of rationality and proportionality are duly respected. Of particular relevance is whether institutions involved in the investigation, prosecution, and adjudication of illicit enrichment are properly monitored, accountable, resourced, and trained so that they are in a position to implement the obligations taken under the International Covenant on Civil and Political Rights and to pursue corrupt money effectively and fairly.[103] In the precedent set by *Salabiaku v. France* the European Court of Human Rights outlined its approach to the permissibility of burden-shifting provisions, as approach that has been referred to as the *Salabiaku* test.[104] The UN Human Rights Council has stated "effective anticorruption measures and the protection of human rights are mutually reinforcing and that the promotion and protection of human rights is essential to the fulfilment of all aspects of an anticorruption strategy."[105]

The World Bank and UNODC point out that freezing or seizure of assets infringes on the property rights of the asset holder, but such action is warranted when balanced against the

[98] Police Federation of Australia and the Australian Federal Police Association, Submission to the Senate Committee on Legal and Constitutional Affairs on *Crimes Legislation (Organised Crime and Other Measures) Bill,* 31 January 2013, pp. 5-7.
[99] Parliamentary Joint Committee on Law Enforcement, 'Inquiry into Commonwealth unexplained wealth legislation and arrangements', March 2012, pp. 30-32.
[100] Parliamentary Joint Committee on Law Enforcement, 'Inquiry into Commonwealth unexplained wealth legislation and arrangements', March 2012, p. xvi.
[101] Lindy Muzila, Michelle Morales, Marianne Mathias and Tammar Berger, 'On the Take. Criminalizing Illicit Enrichment to Fight Corruption', The World Bank and UNODC, Washington, 2012, p. 8.
[102] Lindy Muzila, Michelle Morales, Marianne Mathias and Tammar Berger, 'On the Take. Criminalizing Illicit Enrichment to Fight Corruption', The World Bank and UNODC, Washington, 2012, p. 9.
[103] Lindy Muzila, Michelle Morales, Marianne Mathias and Tammar Berger, 'On the Take. Criminalizing Illicit Enrichment to Fight Corruption', The World Bank and UNODC, Washington, 2012, p. xiv.
[104] Lindy Muzila, Michelle Morales, Marianne Mathias and Tammar Berger, 'On the Take. Criminalizing Illicit Enrichment to Fight Corruption', The World Bank and UNODC, Washington, 2012, p. 31.
[105] UN Human Rights Council Resolution 7/11 of 27 March 2008, on the role of good governance in promoting and protecting human rights.

rights of victims to recover stolen funds and the need to secure funds before the asset holder is tipped off. In addition, safeguards can be introduced to ensure that the asset holder has the opportunity to contest the freezing order.[106]

As noted in the previous Parliamentary inquiry into unexplained wealth legislation, such legislation already exists in Ireland, the US, the UK and Italy.[107]

In addition in Germany, Criminal Code, Section 73d, is enabling legislation that shifts the burden of proof to the accused if the prosecution establishes a significant increase in the assets of a public official that have not been accounted for. The legislation requires forfeiture of assets "where there are grounds to believe that the objects were used for or obtained through unlawful acts." The Federal Supreme Court has argued that this does not reduce the burden of proof but absolves the prosecution from establishing "the specific details" of the offence.[108]

Similarly, Article 36 of the Dutch Criminal Code allows for the confiscation of the proceeds of the crime for which the offender has been convicted as well as the confiscation of assets "which are probably derived from other criminal activities". The Supreme Court has argued that this is consistent with the presumption of innocence because:[109]

> *Once a presumption of criminal origin of proceeds has been established by the prosecution, the defense can always reverse the presumption. Once the criminal origin of the proceeds has been made probable, the burden to rebut – not simply to deny – this presumption lies with the defense.*

In Switzerland if it is established that an individual supports or is part of a criminal organisation, the court is obligated to order the confiscation of all the assets owned by that individual. Criminal Code, Article 59(3), creates a presumption that a criminal organisation controls the assets of all of its members. It is then up to the individual to rebut the presumption by demonstrating the legal origin of the assets. The Supreme Court upheld the position that this respects the presumption of innocence because the accused can rebut it by demonstrating that they are not under the organisation's control or the assets have legal origin.[110]

In 2010 the Swiss Parliament also introduced the *Return of Illicit Assets Act*, which seeks to facilitate the recovery of the proceeds of corruption in situations where the state of origin of the assets is unable to conduct a criminal procedure that meets the requirements of Swiss law on international mutual assistance. This provides for the freezing, forfeiture and restitution of assets held by foreign politically exposed persons (PEPs, a term defined within international anti-money laundering standards) and their associates in Switzerland on the basis of decisions by the Federal Administrative Court. The court may presume the unlawful origin of these assets where:

> *The wealth of the person who holds powers of disposal over the assets has been subject to an extraordinary increase that is connected with the exercise of a public office by the politically exposed person and the level of corruption in the country of origin or*

[106] 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. 55.
[107] Parliamentary Joint Committee on Law Enforcement, 'Inquiry into Commonwealth unexplained wealth legislation and arrangements', March 2012, p. v.
[108] Lindy Muzila, Michelle Morales, Marianne Mathias and Tammar Berger, 'On the Take. Criminalizing Illicit Enrichment to Fight Corruption', The World Bank and UNODC, Washington, 2012, p. 35.
[109] Lindy Muzila, Michelle Morales, Marianne Mathias and Tammar Berger, 'On the Take. Criminalizing Illicit Enrichment to Fight Corruption', The World Bank and UNODC, Washington, 2012, p. 35.
[110] Lindy Muzila, Michelle Morales, Marianne Mathias and Tammar Berger, 'On the Take. Criminalizing Illicit Enrichment to Fight Corruption', The World Bank and UNODC, Washington, 2012, p. 36.

surrounding the politically exposed person in question during their time in office is or was acknowledged as high.

The court may reject the presumption "if it can be demonstrated that in all probability the assets were acquired by lawful means." Decisions of the Federal Administrative Court are subject to appeal to the Federal Supreme Court.[111]

5.2 The Need for Speed, Trust, Transparency and Flexibility

The World Bank and UNODC have pointed out that because assets can be moved within minutes and at the click of a button, investigations need to act in a time-sensitive manner. Any delay in executing a freezing request after the suspect has been arrested or tipped off can be fatal to the recovery of assets. They expressed concerns that the current mutual legal assistance processes are not sufficiently agile to address this reality, particularly for tracing, freezing or seizing of assets. Although many jurisdictions permit mutual legal assistance applications during the investigation stages or once there is reason to believe that a proceeding is about to be instituted against the alleged offender, a few jurisdictions require that criminal charges be initiated before the restraint or seizing assistance can be provided. Practitioners stated to the World Bank and UNODC that this approach impairs efforts to preserve assets by providing notice to the asset holder before the necessary provisional measures have taken place. By the time a response is received to a request to restrain assets, they will have been moved.[112]

They also point out a lack of trust of foreign jurisdictions often has resulted in delays that have allowed criminal assets to move before they can be seized.[113] The Unit notes with concern that there often are groups within Australia who will oppose effective legislation to co-operate with foreign law enforcement agencies on the basis that foreign law enforcement agencies cannot be trusted. The Unit believes instead that effective and timely co-operation should be provided, but with adequate safeguards for human rights and against misuse of the assistance provided.

The World Bank and the UNODC recommend that jurisdictions should have in place mechanisms that allow for prompt tracing and temporary freezing of assets before a formal mutual legal assistance request is filed. A formal mutual legal assistance request would be required to retain the freeze. They make the point that a request for a temporary freeze before charges are laid should be distinguished from a request to forfeit assets, which is permanent and requires notice to the asset holder in most jurisdictions.[114]

They recommend that a requested jurisdiction should not refuse a request for mutual legal assistance around the recovery of stolen assets for due process reasons unless it has precise and strong evidence that the originating jurisdiction has not guaranteed due process to the defendants. Further, they also recommend that developed countries should consider absorbing the costs of communication with developing-country jurisdictions on requests for assistance with recovery of stolen assets.[115]

---

[111] Lindy Muzila, Michelle Morales, Marianne Mathias and Tammar Berger, 'On the Take. Criminalizing Illicit Enrichment to Fight Corruption', The World Bank and UNODC, Washington, 2012, p. 37.
[112] 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. 54.
[113] 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, pp. 19-20.
[114] 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. 55.
[115] 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. 23.

The World Bank and UNODC recommend that requested jurisdictions implement policies and procedures that guarantee transparency when dealing with originating authorities and should require that the reasons for rejecting a mutual legal assistance request relating to recovery of stolen assets be divulged to the originating jurisdiction; they should also give the originating jurisdiction an opportunity to demonstrate that the defendant received due process.[116]

The World Bank and UNODC has recommended that governments effectively address legal barriers by adopting a more flexible and proactive approach to dual criminality (criminalisation of the offence in both jurisdictions) and reciprocity and to take steps to limit the grounds for mutual legal assistance refusal, including by extending statutes of limitation.[117] They also noted that "many judges and prosecutors in some developed jurisdictions continue to consider asset recovery a novelty to be treated with caution. This cautious approach often contributes to time-consuming and ineffective management of processes for repatriating stolen assets, which frequently includes international cooperation."[118]

The World Bank and the UNODC also stress the importance of informal assistance in cases of recovery of stolen assets from foreign jurisdictions involving direct communication between Financial Intelligence Units (FIUs), police and prosecutors of the two jurisdictions to discuss intelligence gathered with the anticipation of a formal mutual legal assistance request to follow. With fewer restrictions, practitioners can gather information more quickly than they can under a formal mutual legal assistance request process, build the necessary substantive foundation for an eventual formal request, and develop a strategy that best accords with the advantages and limitations of both jurisdictions' systems. The importance of these informal channels of assistance and cooperation among counterpart agencies outside the realm of mutual legal assistance has been emphasised in the UN Convention Against Corruption and by the Financial Action Task Force.[119]

5.3 Importance of Non-Conviction Based Restraint and Confiscation

The World Bank and UNODC also point out the importance of having a non-conviction based confiscation and restraint mechanism, arguing that in many instances it is the only way to recover the proceeds of corruption and to exact some measure of justice.[120] In their research they found practitioners highlighted the usefulness of non-conviction based confiscation because it can be quicker and more efficient and may be the only recourse when the offender if dead, has fled the jurisdiction, or is immune from prosecution.[121] The World Bank and the UNODC further argue that it is best not to limit the scope of non-conviction based confiscation and restraint, but at a minimum it should apply to circumstances where the perpetrator is dead, a fugitive, absent or unknown as well as in "other appropriate cases".[122] In addition to having domestic legislation allowing for non-conviction based restraint and

[116] 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. 23.
[117] 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. 3.
[118] 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. 24.
[119] 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. 41.
[120] 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. 66.
[121] 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. 67.
[122] 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. 67.

confiscation of assets, they recommend that jurisdictions should allow for enforcement of foreign non-conviction based restraint orders.[123]

5.4 Examples of Politically Exposed Persons from PNG to whom unexplained wealth provisions may have been appropriate

The following are examples of cases where transfers of assets from PNG to Australia might have been subject to unexplained wealth provisions, if the assets being transferred could not be identified as having a legitimate origin.

5.4.1 Paul Paraka

Paul Paraka, the principle lawyer of Paul Paraka Lawyers, was charged in October 2013 in PNG with 18 counts of allegedly receiving fraudulent payments of $28.7 million.[124] It is alleged that the law firm Paul Paraka Lawyers received these unapproved funds from PNG's Department of Finance.[125] Mr Paraka is facing 18 charges, which include:[126]

- Five counts of conspiracy to defraud the state;
- Nine counts of stealing by false pretence;
- Two counts of money laundering; and
- Two counts of dishonest application of the monies.

The case is being investigated by Fraud and Anti-Corruption Directorate detectives attached to Taskforce Sweep.[127]

Paul Paraka was a customer of NAB, and he had been transferring large sums of money to contacts in Australia (in the Gold Coast and NSW).[128] Investigations by journalists found bank accounts linked to Mr Paraka have transferred nearly $3 million into Australia, including a three-part $80,000 transaction to his Australian-based wives and girlfriends, including one that was living in the Star City Casino complex.[129] It has been alleged that PNG investigators believe that most of the funds were corruptly obtained.[130]

There were serious findings against Mr Paraka by the PNG Government Commission of Inquiry generally into the Department of Finance in their report completed at the end of October 2009. It was alleged by Finance Minister James Marape that senior officers within the department continued to authorise payments to Paul Paraka Lawyers despite being instructed not to do so.[131]

5.4.2 Eremas Wartoto

Eremas Wartoto is a politically connected Papua New Guinean businessman. He was committed to stand trial in absentia.[132]

---

[123] 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. 69.
[124] ABC Australia, 'Papua New Guinea Lawyer Paul Paraka charged over $30 million in fraudulent payments', 24 October, 2013; and Rowan Callick, 'Top PNG lawyer arrested over $28m', *The Australian*, 25 October 2013.
[125] ABC Australia, 'PNG's PM threatens Finance Department', 22 May, 2013.
[126] ABC Australia, 'Papua New Guinea Lawyer Paul Paraka charged over $30 million in fraudulent payments', 24 October, 2013.
[127] 'Cops get boot', *Post Courier,* 13 January 2014.
[128] Nick McKenzie and Richard Baker, 'PNG dirty money trail leads to Australia', *The Age*, July 19, 2013.
[129] Ibid.
[130] Ibid.
[131] ABC Australia, 'Heads roll as major scandal embroils PNG Finance Dept', 23 May, 2013.
[132] Sam Koim, 'Investigation Taskforce Sweep June 2013 Report', *Post Courier,* 2 August 2013, p. 46.

In 2011, Taskforce Sweep charged Mr Wartoto with the misappropriation of $5 million.[133] Mr Wartoto has been charged over the "payment of K7.9m [$3.2 million] of RESI [Rehabilitation Education School Infrastructure] funds allocated for Kerevat NHS [National High School]".[134] On the 30 August 2011, Mr Wartoto was charged; but then obtained an Australian foreign skilled workers visa and fled to Queensland on the 3 September 2011.[135] He was charged with two counts of misappropriation of property of Papua New Guinea in contravention of section 383(1) (a) of the *Criminal Code Act 1974* (PNG). Mr Wartoto claimed that he was 'too ill' to travel back to Port Moresby, despite the fact that he frequently travelled internationally within the two year period that he was in Australia.[136]

On 30 August 2012, PNG authorities issued a restraining order to cover property owned by Eremas Wartoto in PNG.[137]

On 24 April 2013, Papua New Guinea made a 'Mutual Assistance Request' to the Australian Federal Police, asking for assistance in registering a 'Foreign Restraining Order' that was made in 2012 against Mr Wartoto under the *Proceeds of Crime Act 2005* (Papua New Guinea).[138] On the 26 May, 2013, the District Court of Queensland registered the Foreign Restraining Order over Mr Wartoto's five Australian properties and four bank accounts believed to be associated with Mr Wartoto.

The PNG authorities had stated they believed Mr Wartoto engaged in "asset protection measures" in relation to his Australian assets to prevent these being seized under the PNG *Proceeds of Crime Act 2005.* These asset protection measures included the registration of second mortgages over Australian properties in favour of Litia Ilam and Louisah Wartoto as Trustees of the Wartoto PNG trust, which the PNG authorities believed was under the effective control of Mr Wartoto.[139]

The Australian Federal Police (AFP) lodged a successful application to have Mr Wartoto's property seized.[140] The AFP's application to the court was under section 35 of the *Mutual Assistance in in Criminal Matters 1987* (Cth) requesting that the Official Trustee in Bankruptcy take custody and control of property.[141]

The five properties in Queensland owned by Mr Wartoto in Queensland are in:

- Bentley Park, bought for $247,000 in February 2004. It was jointly owned by Eremas Wartoto and Louisah Wartoto and the Westpac Bank provided the mortgage. The mortgage was cancelled on 9 July 2010. The property was gifted to Eremas Wartoto Pty Ltd on 22 June 2010.

[133] Sarah Elks and Rowan Callick, 'Property of PNG fugitive seized', *The Australian,* 15 May 2013.
[134] Sam Koim, 'Investigation Taskforce Sweep June 2013 Report', *Post Courier,* 2 August 2013, p. 46.
[135] Nick McKenzie & Richard Baker, 'Alleged PNG crime boss on 457 visa wanted over theft of $30m', *The Age,* 10 May 2013; and Affidavit filed in Brisbane by the Commissioner of the Australian Federal Police, District Court of Queensland, 7 May, 2013 (number BD 1440/2013).
[136], Nick McKenzie & Richard Baker, 'Alleged PNG crime boss on 457 visa wanted over theft of $30m', *The Age,* 10 May 2013.
[137] Affidavit filed in Brisbane by the Benjamin Ross Moses for the Commissioner of the Australian Federal Police, District Court of Queensland, 6 May, 2013.
[138] Affidavit filed in Brisbane by the Commissioner of the Australian Federal Police, District Court of Queensland, 7 May, 2013.
[139] Affidavit filed in Brisbane by the Benjamin Ross Moses for the Commissioner of the Australian Federal Police, District Court of Queensland, 6 May, 2013.
[140] Sarah Elks and Rowan Callick, 'Property of PNG fugitive seized', *The Australian*, 15 May 2013.
[141] Application filed in Brisbane by Commissioner of the Australian Federal Police, District Court of Queensland, April 26 2013 (number BD1440/2013).

- Edmonton, bought for $540,000 in September 2007. The ANZ bank provided a mortgage. A second mortgage was provided by Litia Ilam and Louisah Wartoto as Trustees of Wartoto PNG Trust on 23 November 2012.
- Cairns, bought for $575,000 in April 2010. Jointly owned with Louisah Wartoto. The ANZ bank provided the mortgage.
- Cairns, bought for $415,000 in November 2010. The ANZ Bank provided the mortgage on the property. A second mortgage was provided by Litia Ilam and Louisah Wartoto as Trustees of Wartoto PNG Trust on 23 November 2012.
- Mount Sheradan, bought for $515,000 in January 2011. The ANZ Bank was the mortgagee. A second mortgage was provided by Litia Ilam and Louisah Wartoto as Trustees of Wartoto PNG Trust on 23 November 2012.

A caveat was placed on each of these titles by the Australian Federal Police (AFP) on 2 May 2013 due to the proceeds of crime legal action being taken by the AFP.

The Wartoto PNG Trust was created on 7 November 2005 for the children and grandchildren of Eremas Wartoto and Louisah Wartoto.

A restraining order was issued by the PNG National Court of Justice on 2 May 2013 for four separate bank accounts, three Westpac accounts in the name of Louisah Wartoto and one in the name of Travel-Car Australia with the Bendigo Bank. Eremas Wartoto also held motor vehicles registered in the names of Travel Car Pty Ltd.

Improvements to Australia's ability to restrain unexplained wealth may have assisted in restraining Mr Wartoto's assets in Australia more quickly and reduced the risk the assets would have been shifted to another jurisdiction.

5.4.3 Jeffery Yakopya

Jeffery Yakopya the former assistant secretary in the PNG National Planning and Monitoring Department was arrested by Taskforce Sweep after allegedly approving a K1,975,006 ($0.89 million) variation claim lodged on behalf of Sarakolok West Transport Ltd (SWT).[142] These funds were on top of an alleged K7.9 million ($3.6 million) paid to SWT, a company owned by Eremas Wartoto.[143] Taskforce Sweep has alleged that Mr Yakopya has misappropriated a total of K16.575 million ($7.5 million).[144] He has been committed to stand trial.[145] Jeffery Yakopya owns one property in Queensland, in Bentley Park, bought for $420,000 in November 2009. A mortgage on the property was provided by the ANZ Bank. It is impossible to know from the outside if the ANZ Bank fulfilled its due diligence requirements under anti-money laundering legislation thoroughly in 2009 in dealing with Mr Yakopya and the funds that were used to repay the mortgage had a legitimate source.

5.4.4 Paul Tiensten

Paul Tiensten was the former Minister for National Planning and Monitoring for PNG and the Member of Parliament for Pomio. In September 2011 he fled to Brisbane after being summonsed by Taskforce Sweep to answer questions over misappropriation of funds at the Department of Planning, and upon returning to PNG was subsequently arrested.[146] Paul Tiensten was charged and committed for trial over the alleged misappropriation of funds from this department, after allegedly diverting funds of approximately K3.4 million ($1.5 million)

[142] Sam Koim, 'Investigation Taskforce Sweep June 2013 Report', *Post Courier,* 2 August 2013, p. 46.
[143] 'Sweep team arrest two more', *The National*, 3 January 2012; and Sam Koim, 'Investigation Taskforce Sweep June 2013 Report', *Post Courier,* 2 August 2013, p. 46.
[144] 'Investigation Taskforce Sweep 2013 Report', *Post Courier,* 2 August 2013.
[145] Sam Koim, 'Investigation Taskforce Sweep June 2013 Report', *Post Courier,* 2 August 2013, p. 46.
[146] Liam Fox, 'Ex-minister arrested on return to PNG', ABC News, 17 November, 2011.

from Mesu Investment Limited intended for the Karalai Plantation Rehabilitation to his family company Tolpot Services Limited.[147]

Paul Tiensten was also charged in relation to dishonestly approving a government grant of approximately K10 million ($4.5 million) to facilitate the set up an airline called 'Travel Air', owned by Eremas Wartoto, despite the money having been earmarked for rural air freight subsidies.[148] He was convicted on this charge and Judge Gibbs Salika said that Mr Tiensten had used his "political muscle" to force the grant through.[149] He was sentenced on 28 March 2014 nine years in prison with hard labour, but four years of the sentence will be suspended if he repays the money.[150]

In 2008, Wu Shih-tsa, a businessman from Singapore, testified in a Taiwan court that six PNG officials had received part of a $19 million bribe, including Paul Tienstein. Paul Tienstein denied knowledge of the bribe. Four years ago, Paul Tiensten was also accused of a $90 million fraud also involving executives of four landowner associations in Gulf province, in which funds were released by the National Planning Office to the groups for infrastructure projects that were never built. The case failed for procedural reasons.[151]

Paul Tiensten's wife Julie Tiensten owned one property in Queensland, in North Quay Brisbane City, bought for $570,000 bought in May 2009. The contact address for Julie Tiensten on purchase of the property was a property owned by Eremas Wartoto in Mt Peter Road, Edmonton. The North Quay Brisbane City property was sold on 14 November 2013 for $455,000. The mortgage on the property in 2009 was provided by the Commonwealth Bank.

6. Combatting Online Commercial Child Sexual Abuse Businesses

There are several hundred online commercial child sexual abuse businesses that produce child sexual abuse material for sale online, with evidence that Australians are accessing and purchasing such material. The Unit urges that Australia takes further steps to combat this form of transnational organised crime.

The Unit will use the terms 'child sexual abuse material' or 'child abuse material' in this section. This reflects the terminology used by those who work with survivors of online child sexual abuse and law enforcement. 'Child pornography' still appears in some international conventions and in early laws written to criminalise the material. Given the growing acceptance of pornography as a legitimate product in Western societies, the term 'child pornography' is now seen to offer some legitimacy to the material in question when it should be regarded as unacceptable and criminal. The term is also used by opponents of the full range of measures needed to remove this material.

The commercial trade in images of child sexual abuse involves hundreds of commercial child sex abuse sites. An estimated 50,000 new child sexual abuse images are produced each

[147] 'Tiensten in custody on second charge', *Post Courier*, 18 November, 2011; and Sam Koim, 'Investigation Taskforce Sweep June 2013 Report', *Post Courier,* 2 August 2013, p. 46.
[148] Liam Fox, 'PNG businessman up on yet more fraud charges', ABC News, 21 May 2013; and Sam Koim, 'Investigation Taskforce Sweep June 2013 Report', *Post Courier,* 2 August 2013, p. 46.
[149] Rowan Callick, 'PNG gets moving on scourge of corruption', *The Australian,* 2 December 2013, p. 9.
[150] 'Tiensten jailed', *Papua New Guinea Post Courier*, 31 March 2014; and Rowan Callick, 'Ex-PNG minister gets nine years' jail', *The Australian,* 1 April 2014, p.7.
[151] Rowan Callick, 'Ex-PNG minister gets nine years' jail', *The Australian,* 1 April 2014, p.7.

year.[152] The industry is estimated to be worth about US$250 million annually globally.[153] Reportedly a single child sexual abuse site can attract up to one million hits monthly.[154]

Organised criminals, mainly in Eastern Europe and increasingly in Asia, run 'businesses' selling images and videos of child sexual abuse online primarily to make money. The purchase and trade in commercial sexual abuse material generates a market and ongoing demand for abuse through the production of the material. Human trafficking particularly feeds the commercial child sexual abuse industry on the Internet.[155]

Children under the age of 18 who are used for commercial sexual purposes are deemed to be victims of human trafficking under the definition in the US *Victims of Trafficking and Violence Protection Act 2000*. The Act defines sex trafficking as "recruitment, harbouring, transportation, provision, or obtaining of a person for the purpose of a commercial sex act."[156]

The commercial child sexual abuse industry is different to peer to peer networks of sex offenders who share images but do not seek to make a profit. The primary objective of the commercial industry is to sell images of child sexual abuse in order to make a profit. These commercial networks are more likely to involve younger children than peer to peer networks.

The UN Office of Drugs and Crime (UNODC) have found the majority of commercial child sexual abuse operations are located in Eastern Europe. This is due to lower levels of law enforcement in Eastern Europe targeting this criminal activity and because the customers, who are largely from Western countries, have a preference for 'white' girls.

Commercial websites tend to cater to a specific group of offenders. They often have higher levels of extreme sexual abuse and sexual torture of children than images on non-commercial sites. Images are grouped in specific or narrow age ranges including categories for infants and toddlers, although this was a minority.[157] Just under a third of the images (29.7%) depict children being sexually assaulted, with 3.3% of images on commercial sites being of extreme sexual assaults compared to 2.7% of images on all child sexual abuse websites.

Trend data from the UK Internet Watch Foundation has found, disturbingly, the proportion of images of victims of child sexual abuse under the age of 10 increased from 74% in 2011 to 81% in 2012.[158] At the same time the proportion of images of child sexual abuse showing sexual activity between adults and children including rape and sexual torture decreased from 64% of images in 2011 to 53% of images in 2012.[159]

Offenders accessing child sexual abuse material use a variety of online methods. One study found, of a sample of offenders, 78% obtained images using Internet Relay Chat software,

---

[152] UNODC, *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* on 17 June 2010
[153] [i]bid.
[154] R. Wortley, Child Pornography. In: Natarajan M, editor. *International crime and justice*. USA: Cambridge University Press, 2010, p.178-84, cited in J. Pritchard et.al, 'Internet subcultures and pathways to the use of child pornography', *Computer Law and Security Review* 27, 2011, p.589
[155] UNODC, *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* on 17 June 2010
[156] Catherine Marcum and George Higgins, *Combating Child Exploitation Online: Predictors of Successful ICAC Task Forces,* Policing **5(4)**, p. 310.
[157] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, p. 41.
[158] Internet Watch Foundation, 'Internet Watch Foundation Annual and Charity Report 2012', p. 11.
[159] Internet Watch Foundation, 'Internet Watch Foundation Annual and Charity Report 2012', p. 11.

42% used the World Wide Web, 39% used newsgroups, 30% e-mail and 21% ICQ.[160] This sample included offenders who both shared images and those that purchased images, so it was not restricted only to offenders that purchase images from commercial child sexual abuse operations.

The UK Internet Watch Foundation report the make-up of the top 10 types of websites on which child sexual abuse material is hosted are:

- Image host (45%)
- Banner site (12%)
- Social networking site (12%)
- Generic websites (10%)
- File host (6%)
- Image Store (5%)
- Image Board (4%)
- Forum (3%)
- Web archive (2%)
- Blog (< 1%)

Commercial sites also rely on selling to a large number of customers, as this allows the sale price to be lower. It also means more revenue can be obtained for each image and the risk of detection and apprehension by law enforcement is reduced, as the production of each image involves greater risk of being caught by law enforcement. The Internet Watch Foundation report there has been a change in the way child sexual abuse material is hosted on the internet with a growing amount of content being posted to separate locations rather than large collections of images stored within a folder on a single website.[161]

Since 2009, the Internet Watch Foundation identified 998 unique sources of commercial child sexual abuse websites, each with a distinct website name and brand. They found 321 of these were active in 2010, 440 were active in 2011 and 513 were active in 2012. Of the 513 commercial child sexual abuse brands active in 2012 that were detected by the Internet Watch Foundation, 268 were new brands.[162] Of these, the ten most prolific 'brands' account for at least 47.7% of the commercial webpages seen by the Internet Watch Foundation, with the most prolific using 862 URLs. Within the top 30 brands, no new 'top level' brand was identified in 2011.[163] They found of the top 30 most prolific 'brands' of commercial child sexual abuse material active in 2012, 16 of these appeared to be associated with a single 'top level' distributor.[164] Of the 9,550 child sexual abuse webpages detected by the Internet Watch Foundation in 2012, 2,587 (27%) were commercial sites.[165]

[160] A.R. Beech, I.A. Elliott, A. Birgden, and D. Findlater, *The internet and child sexual offending: A criminological review,* Aggression and Violent Behaviour **13** (2008), 226.
[161] Internet Watch Foundation, '2010 Annual and Charity Report', p. 8.
[162] Internet Watch Foundation, 'Internet Watch Foundation Annual and Charity Report 2012', p. 16.
[163] Internet Watch Foundation, '2011 Annual and Charity Report', p. 15.
[164] Internet Watch Foundation, 'Internet Watch Foundation Annual and Charity Report 2012', p. 16.
[165] Internet Watch Foundation, 'Internet Watch Foundation Annual and Charity Report 2012', p. 16.

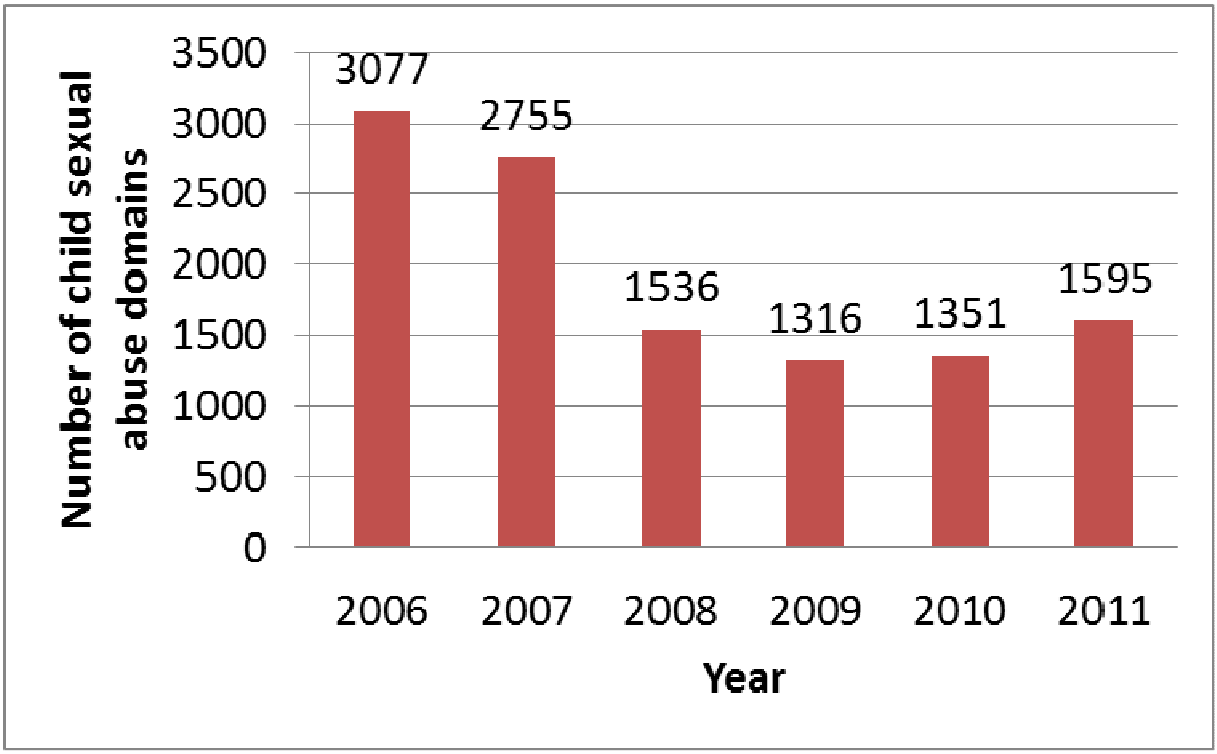

Figure 1. Number of child sexual abuse domains detected by the UK Internet Watch Foundation 2006 – 2011.[166]

The Internet Watch Foundation reports that in the last two years they have seen an increasing number of legitimate websites being criminally exploited to host child sexual abuse material.[167]

The UK Internet Watch Foundation reported in 2012 there were 26 URLs of child sexual abuse material hosted within hidden services. This is achieved through the use of proxy software that conceals the location of the web server hosting the content, making removal of the content at source impossible.[168]

Commercial sites are also supported by a range of payment methods to help avoid detection.[169] Payment systems may involve pre-pay cards, credit cards, 'virtual money' or e-payment systems and may be carried out across secure webpages, text or e-mail. A report by Cybetip.ca identified 27 different payment types.[170] The majority (85%) sold memberships, with recurring monthly payments ranging from $4 to $490 (an average of $53 a month). Membership could also be obtained for a one-time fee ranging from $30 to $1,990[171] with an average cost of $249.[172] DVDs were also sold for as much as $1,900. Other products include

[166] Internet Watch Foundation, '2011 Annual and Charity Report', p. 12.
[167] Internet Watch Foundation, '2011 Annual and Charity Report', p. 13.
[168] Internet Watch Foundation, 'Internet Watch Foundation Annual and Charity Report 2012', p. 17.
[169] Analysis by the Internet Watch Foundation (Annual and Charity report p.8) has identified that the criminals running these operations do so in a cluster of commercial child sexual abuse 'brands' from the manner in which they share hosting patterns, payment arrangements, advertising systems and registration details as well as from the overall appearance of the websites.
[170] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, pp. 10, 56.
[171] This type was used by 15.4% of the sites.
[172] Canadian Centre for Child Protection, *op.cit*. p. 65.

a variety of packages, image sets, videos and websites.[173] They concluded there is clearly a large consumer market for child sexual abuse images.

A UK commercial online child sexual abuse operation was estimated to have made £2.2 million through the distribution of millions of images. Their pages contained 121,654 images of child sexual abuse. Police were able to identify 1,511 suspected customers of the criminal operation.[174]

In addition to the commercial child sexual abuse sites there are many sites that do not have their own commercial component but exist for the purpose of promoting commercial sites. In providing links, re-directs or advertisements for distinct commercial websites, these sites may receive payment or reciprocal linking for making child sexual abuse material available. These websites indirectly profit from the sale of child sexual abuse images.[175]

In addition, the Internet Watch Foundation reported in 2011 they had discovered a cluster of commercial (and some non-commercial) sites that can only be accessed via a predetermined 'digital path'. These 'disguised websites' present different content based on the route the user takes. When the URL is loaded directly into a browser, the page that loads usually contains legal adult content. However, if the same website is accessed via a particular gateway (referrer), the site displays child sexual abuse images. This technique means a commercial child sexual abuse operator may be able to acquire legitimate business services, such as banking services, if the website appears to host legal content when directly accessed. It also means that if the site is reported to law enforcement without the person reporting it also reporting the path to the illegal content, it will appear to be a false report to the law enforcement agency. The Internet Watch Foundation have developed a technique to circumvent the digital 'footpath' to gain access to the child sexual abuse content. The Internet Watch Foundation detected the use of this technique on 579 occasions during 2011.[176]

The supply chain for child sexual abuse material entering Australia involves the following links:

- The producers of the child sexual abuse material, be it photos or video;
- The content host, that makes the material accessible online;
- The Internet Service Provider that allows the customer to access the material;
- The offender purchasing the material; and
- The body or bodies that provide the payment system that allows the producer to get paid for the material.

Actions can be taken against each link in this supply chain. In each case, counter strategies are available to offenders to try and circumvent actions to combat the commercial child sexual abuse trade.

The actions that the Australian Government can be taken at each step in the chain are:

- **Producers**
    - Assist in the identification and location of those involved in the production so that law enforcement in the country they are located in can arrest and prosecute them.
    - Assist in the identification and location of their victims, so the victims can be rescued.

[173] DVDs accounted for 5.8% of the sites, packages 4.7%, image sets 3.1%, videos 1.1% and websites 0.2%.
[174] Child Exploitation and Online Protection Centre, "Operation Alpine: Four main suspects sentenced today", 13 June 2011; and "Three jailed over £2.2 million internet child porn business", The Daily Mirror, http://www.mirror.co.uk/news/uk-news/three-jailed-over-22million-internet-134758.
[175] Canadian Centre for Child Protection, *op.cit*, p. 56.
[176] Internet Watch Foundation, '2011 Annual and Charity Report', p. 15.

- **Content Hosts**
  - Enforce the offence of knowingly hosting child sexual abuse material.
  - Ensure that URLs and domains that have been used by commercial child sexual abuse operations are deregistered and cannot be used again.
  - Support the roll out of new technologies, such as Microsoft's Photo DNA, that can be used to remove known images of child sexual abuse material.
- **Internet Service Providers (ISPs)**
  - Enforce the offence of knowingly providing service to child sexual abuse material.
  - Enhance disruption of access to child sexual abuse sites through the mandatory requirement to block ready access based on a URL or domain list of child sexual abuse sites and domains. It may also be possible to disrupt access to child sexual abuse material through filters that use the filehash value of the images.
- **'Customers'**
  - Enforcement of existing offences for possession and trading in child abuse material.
  - Explore catered rehabilitation programs for non-contact offenders where there are sufficient numbers to justify such programs to reduce recidivism.
  - Explore the provision of a help service for offenders who recognise they have a problem and wish to seek help in ending their offending behaviour. This can be advertised through the 'Stop' message tied to ISP level access disruption.
- **Payment Providers**
  - Ensure that financial institutions deny the provision of credit card merchant facilities to any commercial child sexual abuse material provider.
  - Encourage frinancial institutions to work with the Australian Federal Police and the Financial Coalition Against Child Pornography to identify known transaction patterns that would indicate a client is purchasing child sexual abuse material.

6.1 Scale of the problem

Whilst there is an emerging market it in Asia, it is predominantly in western countries where the market exists. According to the available data,[177] hundreds of thousands of people in western democratic societies access child sexual abuse material online either inadvertently or deliberately. In a 2008 survey of 1,000 adults in the UK, the Internet Watch Foundation found that 5% of all internet users had been exposed to child sexual abuse material online.[178] A BBC report from 2006 indicated that UK ISP BT were blocking 35,000 attempts to access child sexual abuse material each day by their clients. [179] At the time, BT provided service to one third of UK internet users. Cybertip.ca also reported that in the UK, a single ISP blocked more than 20,000 daily attempts to access child sexual abuse material and in Norway the estimate was 15,000 – 18,000 daily attempts.[180]

The Asia-Pacific Financial Coalition Against Child Pornography report that Cybertip are receiving more complaints about online child sexual abuse material from within the Asia-Pacific region. In addition, Cybertip is reporting that the Electronic Service Provision (ESP) industry is becoming far more active in reporting matters related to online child sexual material (see Table 1)

[177] Most ISPs that voluntarily block ready access by their clients to child sexual abuse material either do not collect data on the number of attempts made by clients or do not report this statistic.
[178] Internet Watch Foundation, 'UK adult internet users: 2008 research report', http://www.iwf.org.uk/resources/research
[179] http://news.bbc.co.uk/1/hi/uk/4687904.stm
[180] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, p. 16.

Table 1. Public versus ESP reports to the Cybertip line 2006 to 2013.

Year	2006	2007	2008	2009	2010	2011	2012	2013
Public	44,419	69,414	68,869	58,498	69,280	70,623	60,832	84,238
ESP	32,165	35,847	33,160	61,055	154,094	250,339	348,457	421,042
Total	76,584	105,261	102,029	119,547	223,374	320,962	409,289	505,280

Between 1 July 2011 and 15 October 2011 Telstra blocked 84,000 attempts by Australians to access the child sexual abuse domains on the INTERPOL list of known child sexual abuse domains.

Operation Centurion was triggered after a hacker infiltrated a respectable European website and inserted 99 degrading and explicit images of young girls from eastern Europe, the US and Paraguay. The site was then subject to 12 million hits in just 76 hours after word got around online networks that the images were available and the website's address was circulated. Almost 150,000 different computer users from 170 countries accessed the otherwise obscure website, including Australians using 2,883 computer IP addresses. Of those, 1,513 had downloaded one or more images in the 76-hour period.[181]

US CyberTipline refers attempts to access child sexual abuse images to law enforcement agencies. Between 2006 and 2010 the US CyberTipline made 3,113 child sexual abuse material referrals to Australian law enforcement agencies, compared to 289 to Hong Kong, 603 to New Zealand, 1,765 to Thailand and 5,658 to Japan.[182] Between 2006 and 2013 11,934 referrals were made to Australian law enforcement agencies.

Table 2. CyberTipline referrals of attempts by Australians to access child sexual abuse material online 2006 – 2013.

Year	2006	2007	2008	2009	2010	2011	2012	2013	Total
Number of Referrals	198	228	306	517	1,676	2,760	2,959	3,290	11,934

The available data suggests Australians are also significant consumers of online child sexual abuse material.

In the 2010 – 2011 financial year, law enforcement in Australia charged 112 offenders with offences related to the possession, production or supply of child sexual abuse material.[183] Table 3 outlines prosecution for use of a carriage service for child pornography material or child abuse material, with the data for prosecutions from the Commonwealth Director of Public Prosecution.[184] This does not include additional prosecutions at State and Territory level. The submitting bodies note the current difficulty of trying to collect arrest and prosecution data across States and Territories, as demonstrated by the Commonwealth's own difficulty in trying to provide the data this year to the UN Committee on the Rights of the Child for their review of Australia's implementation of the *Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography.*

[181] Tom Allard, "Child sex abuse: Centurion's shocking fact file", *The Sydney Morning Herald*, 5 June 2008, http://www.smh.com.au/articles/2008/06/05/1212258967845.html.
[182] International Centre for Missing and Exploited Children,' Financial Coalition Against Child Pornography. Building a Global Network', Visa Security Summit, Jakarta, Indonesia, 24 May 2011.
[183] http://www.afp.gov.au/media-centre/fact-stats/online-child-sex-offences.aspx
[184] Commonwealth Director of Public Prosecutions submission to the Joint Select Committee on Cyber-Safety inquiry into Cyber Safety, 2010, p. 5.

Table 3. Prosecutions in Australia for use of a carriage service for child pornography material or child abuse material.

Financial Year	2005/2006	2006/2007	2007/2008	2008/2009	2009/2010
Number of Convictions	2	31	48	126	136

In the data provided in 2012 to the UN Committee on the Rights of the Child:

- Victoria reported 393 offences in the 2009 – 2010 financial year related to possessing or making child sexual abuse material, but no data was provided on the number of offenders involved;
- Western Australia reported 173 files were received in 2011 that related to child sexual abuse material and 28 offenders were arrested. 107 of the files are still under investigation.
- South Australia reported 339 offences related to child sexual abuse material and 205 cases being finalised in SA criminal courts, with a conviction rate of 49.3% for the 2009-2010 financial year.
- NSW reported 81 convictions in 2010 for offences related to production, dissemination or possession of child sexual abuse material.

As an example of Australians buying child sexual abuse material from commercial providers, in mid-November 2013 a joint police operation across borders busted a Canadian commercial child sexual abuse business making and selling 9,000 'movies' and more than 350,000 images of abuse. The business had revenues in excess of $4 million. The Toronto owner of the business was arrested by Canadian police. Sixty-five Australian customers of the site were arrested by Australian police and 399 charges were laid against them. In addition 386 children globally were rescued from exploitation.

Due to the size of the problem and limited resources by comparison, police usually catch offenders who download child sexual abuse material after they have built substantial collections. UK research found that 56% of a sample of 72 offenders who had been caught collected more than 50 images, while 24% of the sample had collections of over 1,000. Two offenders had collections of over 30,000 images and one had a collection of over 80,000 images of child sexual abuse.[185] McCarthy's (2010) study of US offenders who had been caught found the average size of collections of child sexual abuse images and videos for contact offenders was 3,400 compared to 860 for non-contact offenders. In the sample of offenders in McCarthy's study, the offender with the largest collection had 50,150 child sexual abuse images and videos. This again points to the need for interventions that address offending or potential offending behaviour earlier.

INTERPOL manages the International Child Sexual Exploitation Image Database (ICSE DB), which was launched in March 2009. The ICSE DB contains more than 500,000 images of child sexual abuse and is available to certified investigators in any member country in order for them to analyse and share data with colleagues in other countries. By the end of 2009, 1,453 child abuse victims had been identified and rescued worldwide based on the information contained in the ICSE DB.[186] Most victims remain unidentified.

[185] J. Osborn, I.A. Elliott, D. Middleton and A.R. Beech, *The use of actuarial risk assessment measures with UK internet child pornography offenders*, J. of Aggression, Conflict and Peace Research **2(3)** (2010), p. 21.

[186] Weixiao Wei, 'Online Child Sexual Abuse Content: The Development of a Comprehensive, Transferable International Internet Notice and Takedown System', UK Internet Watch Foundation, pp. 61-62.

6.2 Impact of existing efforts

A combination of the above measures globally has already been yielding detectable results in removing commercial child sexual abuse material. According to the UK Internet Watch Foundation, the average length of time child sexual abuse images are hosted has been reduced from years to just days[187] as a result of the above measures. The webpage blocking list maintained by the Internet Watch Foundation now typically contains 600 URLs at any one time, down from 1,200 in 2008.[188] Further, in 2006 the common subscription price to commercial child sexual abuse sites was $30 a month. Today, due to the combination of efforts to shut down and disrupt these criminal enterprises, it is not unusual to find sites that cost up to $1,200 per month and it is rare to find sites charging less than $100 per month.[189]

Removal

Global efforts are being made to have child sexual abuse material removed when it is detected. Law enforcement and regulatory authorities in different countries collaborate to issue 'take down' notices to content hosts to remove child sexual abuse material. The Australian Communication and Media Authority (ACMA) already issues such notices to content hosts for content hosted in Australia. The content must generally be taken down by 6 pm the next business day. Failure to comply may result in the commission of an offence. The ACMA has reported that it has had complete industry compliance with its actions to remove such content.[190]

The Canadian Cybertip.ca has received close to 25,000 reports resulting in 2,800 websites being shut down, at least 30 arrests and the removal of a number of children from abusive environments.[191]

The UK Internet Watch Foundation has reported 50% of all non-UK hosted child sexual abuse URLs occurs within 10 days of detection. When the content of hosted by an Internet Watch Foundation member, 85% is removed within 10 days and 95% within 13 days.[192]

An assessment commissioned by the UK Internet Watch Foundation concluded:[193]

> *There is compelling evidence that domestic notice and takedown systems adopted in some countries are beneficial in effectively removing child sexual abuse content at source without compromising the simultaneous capture of evidence necessary to investigate and prosecute offenders.*

However, the Financial Coalition Against Child Pornography reports "Bulletproof Hosting" is being used to defeat the system of take down notices. These hosts promise customers their websites will not be taken down, regardless of complaints or content. Bulletproof hosts use a

[187] Internet Watch Foundation, '2010 Annual and Charity Report', p. 1.
[188] http://www.iwf.org.uk/resources/trends
[189] International Centre for Missing and Exploited Children and National Centre for Missing and Exploited Children, 'Financial Coalition Against Child Pornography Backgrounder', July 2011, p. 2.
[190] Australian Law Reform Commission, 'Classification – Content Regulation and Convergent Media', ALRC report 118, February 2012, p. 291.
[191] Kim-Kwang Raymond Choo, 'Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences' Australian Institute of Criminology Research and Public Policy Series 103, 2009, p. 70.
[192] Internet Watch Foundation, "2011 Annual and Charity Report", pp. 5, 16.
[193] Weixiao Wei, 'Online Child Sexual Abuse Content: The Development of a Comprehensive, Transferable International Internet Notice and Takedown System', UK Internet Watch Foundation, p. 2.

combination of distributed services to maintain uptime for their customers. Specific tactics they use include:[194]

- Registering the domain name with a registrar with relaxed enforcement. Depending on the location and enforcement policies, some registrars are used more heavily than others for illicit activities.
- Sharing and shuffling IP addresses to minimise downtime if particular IPs are shut down. This ensures content remains up while being indifferent to the status of particular domains. Instead of relying on one IP, bulletproof hosting relies on multiple IPs that can keep the content up independent of specific IP shut downs.
- Using a standardised yet specific naming methodology for name servers to minimise service interruption.
- Soliciting business and communicating with customers using unmonitored, private media. Bulletproof hosts frequently advertise their services on message boards frequented by their target customer base. From there, e-mail, instant messaging and other non-public options are used to further business dealings. This allows bulletproof hosting services to remain largely underground and reduces exposure to enforcement entities.
- Collecting payment using unregulated payment services to limit scrutiny and preserve anonymity. The use of small payment processors originating from outside the US is popular due to lax regulatory environments and lessened cooperation with law enforcement agencies.

Cybertip.ca has made recommendations for content hosts to combat child sexual abuse online including:

- That governments should work together to establish international standards for the personal information a registrant is required to provide when registering a new domain name. This could include proof of name and address, residency in a particular country and contact information. This information could be valuable in the event of an investigation, assisting in determining the owner of a child sexual abuse website, and potentially rescuing children from ongoing sexual abuse.[195]
- Governments should require domain name registrants to discard from use domains hosting illegal content. This would prevent new website owners from purchasing domains known to host child sexual abuse material and reusing them for the same purpose. Due to the fact that the domain names become important marketing tools, and become well-known to consumers of child sexual abuse images, steps need to be taken to remove them permanently from circulation.[196]

Reporting

The ACMA reported that since 2000 it has dealt with 29,029 complaints which have identified 14,441 items of child sexual abuse material online. The UK Internet Watch Foundation hotline dealt with 48,702 reports in 2010.[197]

Research from other jurisdictions suggests a minority of people report even the worst types of material. In a 2008 survey of 1,000 adults in the UK, the Internet Watch Foundation found

[194] Financial Coalition Against Child Pornography, 'Report on Trends in Online Crime and Their Potential Implications in the Fight Against Commercial Child Pornography', 1 February 2011, pp. 12-13.
[195] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, p. 48.
[196] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, p. 49.
[197] Internet Watch Foundation, '2010 Annual and Charity Report', p. 8.

that 5% of internet users had been exposed to child sexual abuse material online.[198] Of those exposed to this material 6% reported it to the police, 4% to their ISP, 4% to a charity, 11% to a hotline that deals with such material, 47% ignored it and 30% said they would have reported it, but did not know how to do so.

In 2012, UK Internet Watch Foundation found 40% of people said they would not know where to report child sexual abuse material online if they encountered it, while 12% said they would simply ignore it.[199] The survey of 2,058 adults in the UK found 4% of men and 2% of women had inadvertently accessed child sexual abuse material online.[200]

PhotoDNA

PhotoDNA is an image matching technology developed by Microsoft which creates a unique 'signature' for a digital image, like a fingerprint. This can be compared to signatures of other images to find copies of the image.

The National Centre for Missing and Exploited Children creates PhotoDNA signatures of the worst known images of child sexual abuse online – images which capture the act of rape via physical penetration of an identified prepubescent child – and shares those signatures (never the images themselves) with online service providers like Facebook to help disrupt the redistribution of those images online. Face Book reported a 65% drop in the hosting of child sexual abuse material after they implemented the use of PhotoDNA to locate such material.

This technique is known in the technology industry as "hashing", but PhotoDNA's 'robust hashing' differs from other common hashing technologies because the signature is based on the essence of the image and not the file. Therefore, if an image has been resized, recolored, saved in a different file format or otherwise similarly altered, PhotoDNA can still reliably identify copies of the same image when other hashing technologies that require every file characteristic to be precisely the same could not.

In March 2012, Microsoft made PhotoDNA available to law enforcement worldwide at no charge to support child sex abuse investigations and help law enforcement more quickly identify and rescue victims and bring their abusers to justice. Law enforcement can now get PhotoDNA source code through direct licensing or in select tools they already use, including NetClean Analyze or the Child Exploitation Tracking System (CETS).[201]

Twitter has started to use PhotoDNA to filter out child sexual abuse material.

In 2003, Microsoft designed a new software known as "CETS" which supports criminal investigators to efficiently organise and share media they come across during investigations. It allows units from various countries to effectively classify track and identify links between indecent material, enabling them to identify owners and uncover international child-porn syndicates. The tool is now in use in seven countries by over 400 investigators worldwide, with demand growing. Microsoft offers the program to interested law enforcement agencies free of charge and donates all training and server software required to deploy the application at no cost.[202]

---

[198] Internet Watch Foundation, 'UK adult internet users: 2008 research report', http://www.iwf.org.uk/resources/research

[199] Internet Watch Foundation, 'New study reveals child sexual abuse content as top online concern and potentially 1.5m adults have stumbled upon it', http://www.iwf.org.uk, 18 March 2013.

[200] Internet Watch Foundation, 'New study reveals child sexual abuse content as top online concern and potentially 1.5m adults have stumbled upon it', http://www.iwf.org.uk, 18 March 2013.

[201] Microsoft PhotoDNA Fact Sheet

[202] Jeffrey Avina, *Public-private partnerships in the fight against crime: An emerging frontier in corporate social responsibility,* Journal of Financial Crime **18(3)** (2011), pp 289-290.

In the Australian Government's response to the UN Committee on the Rights of the Child in their review of Australia's compliance with the *Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography* the Government stated:

> *As part of a national strategy under the auspices of the Australian and New Zealand Police Advisory Agency (ANZPAA) Child Protection Committee, work is progressing on the trial of internet technology that aims to reduce the flow of child exploitation material across the internet within Australia. This technology utilises the known hash values of offending images as a means of identifying inappropriate content being exchanged on peer to peer networks. Work is also progressing on the introduction of the national Child Exploitation Tracking System (CETS), which will enable seizures of child exploitation material to be analysed and compared against known holdings.*

There is an ability to disrupt access on the filehash values of child sexual abuse images. Each image has a unique filehash value and it is possible to block the transmission of images where the filehash value is known. This can be used to disrupt peer-to-peer transmission of images. Currently this technology is used by law enforcement to reduce the number of images they need to view when they catch an offender. The offenders collection of images is run against a database of filehash values of known child sexual abuse images. This means only images not currently in the database must be viewed by police officers. The use of this technology may assist in combating commercial operations that have moved to more individualised sale of images than from a website. It is unlikely to have much impact in deterring networks of contact offenders who will seek counter strategies to defeat it, given their committed sexual interest in children. However, the technology could be adapted to be used as a detection technology to identify offenders trading in known child sexual abuse images for investigation, arrest and prosecution.

Google has also developed a way of 'tagging' child sexual abuse videos so that they can be identified and removed.

Microsoft, Face Book and Google are all working on technology to provide video DNA to assist in the identification of child sexual abuse videos online.

Access Disruption at ISP Level

In their extensive review of classification of media content in Australia, the Australian Law Reform Commission (ALRC) has recommended ISPs be required to disrupt access to 'Prohibited Content' which includes child sexual abuse material.[203] The ALRC suggested that particular subcategories of Prohibited content could be prioritised in ISP access disruption, particularly actual child sexual abuse and non-consensual sexual violence.[204]

In response, the Australian Federal Police have issued notices to ISPs under Section 313 of the *Telecommunications Act,* which requires Australian ISPs to disrupt access to child sexual abuse material using the INTERPOL domain list of the 'worst of' child sexual abuse material. This means the vast majority (90%) of Australians using the internet are no longer able to readily access images of children being sexual abused on domains on the INTERPOL list. It is unlikely that this mechanism will ever achieve 100% coverage of Australian ISPs as there are an estimated 400 to 600 ISPs operating in Australia. However, only 97 of those have more than 1,000 clients. At the same time there are ISPs that made it publicly clear they will not disrupt their clients' ready access to child sexual abuse material unless forced to do so.

[203] Australian Law Reform Commission, 'Classification – Content Regulation and Convergent Media', ALRC report 118, February 2012, Recommendation 5-7 pp. 12, 286, 379.
[204] Ibid. p. 297.

The INTERPOL General Assembly passed a resolution in 2009 (AG-2009-RES-05) stating that it:

> *Encourages member countries to promote the use of all the technical tools available, including access-blocking of websites containing child sexual abuse images, in order to intensify the fight of their national specialised units against the dissemination of child sexual abuse images on the internet;*
>
> *Encourages member countries to systematically provide the INTERPOL General Secretariat with updated lists of websites containing child sexual abuse images for dissemination to INTERPOL member countries, so as to enable them to take appropriate action;*
>
> *Tasks the INTERPOL General Secretariat to maintain and disseminate to the National Central Bureaus a worldwide list of URLs (Internet addresses) which contain those websites that publish the most severe child abuse material.*

INTERPOL has promoted a limited form of domain blocking by ISPs, at the same time noting that existing efforts by some countries to block access to child sexual abuse materials has had "very good results".[205] As of 25 October 2011 the INTERPOL 'worst of' list contained 409 domains.[206]

INTERPOL requires that all the domains on the list be verified as containing child sexual abuse material by at least two different governments/ agencies under the CIRCAMP umbrella. The domain to be blocked must fit the following criteria:

- The children are real. Sites containing only computer generated, morphed, drawn or pseudo images are not included.
- The ages of the children depicted in sexually exploitative situations are (or appear to be) younger than 13 years.
- The abuses are considered severe by depicting sexual contact or focus on the genital or anal region of the child.
- The domains have been online within the last three months.

The method results in over-blocking as the whole domain is deemed illegal if any part of it is found to contain sexual abuse material with children. However, the fact the material has to have been on the domain for three months suggests the domain administrator is not serious about monitoring the content of the domain, and this is a method to force them to act. However, the tight criteria of this form of access blocking reduces its effectiveness as a dynamic disruption strategy against the commercial child sexual abuse industry (compared to the Internet Watch Foundation who update their list of URLs to be blocked twice a day).

INTERPOL argue the "primary goal of blocking access to child sexual abuse material is to protect the rights of the children being depicted, while the secondary goal is to prevent illegal viewing, possession and distribution of the said material." They argue blocking access to child sexual abuse material also has additional benefits:

> *Utilising access blocking will free up resources within the police to work on identifying the victims of child sexual abuse rather than handling recurring reports from the public or NGOs about content being redistributed again and again on commercial web pages. In addition, an overview of the material distributed on the Web pages may provide important evidence and clues in identification cases and can complement ongoing investigations.*

[205] http://www.interpol.int/Public/THBINternetAccessBlocking/
[206] Senate Standing Committee on Legal and Constitutional Affairs. Australian Federal Police Question No 25.

INTERPOL also point out that access blocking assists law enforcement in prosecuting offenders accessing child sexual abuse material as those offenders who circumvent the blocking will then be barred from "using the 'accidental and unwilling access' argument if detected by the police."

They summarise the advantages of access blocking as:

> *The system prevents crimes from being committed, limits the number of criminals having to be investigated in cases related to commercial child sexual abuse material web pages and protects victims. By preventing crime and thereby reducing the amount of work for the police, more resources can be put into investigations and subsequent court proceedings.*

INTERPOL acknowledges that access blocking:

> *…. must be used in combination with traditional police methods, such as investigations into and the removal of child abuse material hosted on the Internet, undercover operations, arrests, searches etc. Blocking child sexual abuse material should never be used instead of the above methods, it should be used in addition to these – in a holistic approach to combat sexual exploitation.*

In the UK, the Internet Watch Foundation reports that its 76 ISP, search and content providers, mobile operators and filtering companies who block client access to child sexual abuse material now cover 98.6% of residential broadband connections.[207]

During 2010 there were a total of 14,602 webpages that featured on the UK Internet Watch Foundation blocking list of live child sexual abuse content. In 2011 this number decreased to 12,966 URLs, hosted in 39 countries.[208] An average of 59 webpages were added to the list each day in 2010, 45 new URLs were added each day in 2011 and 37 new URLs were added each day in 2012, reflecting the speed at which child sexual abuse content moves online location.[209] The webpage blocking list now typically contains 580 URLs at any one time, down from 1,200 in 2008.[210] They update their list twice a day.[211] The Internet Watch Foundation report their entire operation ran on a budget of just £1 million ($1.5 million) in 2009, 2010 and 2011.[212]

The Internet Watch Foundation reported that in 2011 and 2012 it did not receive a single complaint from content owners concerned that they had included in their URL list legitimate content.[213] This demonstrates that it possible to maintain a highly dynamic block list without legitimate content being mistakenly placed on the list.

The Internet Watch Foundation has also publicly announced they are examining the feasibility of extending their operations globally to become Internet Watch Foundation International. This would include offering their URL block list to ISPs internationally.[214]

---

[207] Internet Watch Foundation, '2010 Annual and Charity Report', p. 4; and Internet Watch Foundation, '2011 Annual and Charity Report', p. 17.
[208] Internet Watch Foundation, '2011 Annual and Charity Report', pp. 12-13.
[209] Internet Watch Foundation, '2010 Annual and Charity Report', p. 4; Internet Watch Foundation, '2011 Annual and Charity Report', p. 17; and Internet Watch Foundation, 'Internet Watch Foundation Annual and Charity Report 2012', p. 21.
[210] Internet Watch Foundation, '2011 Annual and Charity Report', p. 17; and Internet Watch Foundation, 'Internet Watch Foundation Annual and Charity Report 2012', p. 21.
[211] Internet Watch Foundation, '2010 Annual and Charity Report', p. 4.
[212] Internet Watch Foundation, '2010 Annual and Charity Report', p. 16; and Internet Watch Foundation, '2011 Annual and Charity Report', p. 22.
[213] Internet Watch Foundation, '2011 Annual and Charity Report', p. 20; and Internet Watch Foundation, 'Internet Watch Foundation Annual and Charity Report 2012', p. 21.
[214] Internet Watch Foundation Strategic Plan 2012-2015.

The Unit urges that the Australian Government seek to extend ISP level access disruption to all the online child sexual abuse sites contained on the UK Internet Watch Foundation, using the UK Internet Watch Foundation list as well as the INTERPOL domain list.

Arrest and Prosecution

Arrest and prosecution of those producing and consuming child sexual abuse material is believed to deter others seeking to access such material. It is a vital tool in the struggle against online child sexual abuse material, but it alone cannot be relied upon as the only response. As the Virtual Global Taskforce of law enforcement agencies has stated many times "law enforcement cannot prosecute itself out of the online sexual exploitation of children alone."[215]

There are no Australian studies publicly available about the number of Australians accessing child sexual abuse material, nor the trend in these numbers. Therefore, it is impossible to provide any comment on how effective arrest and prosecution is in deterring consumption of child sexual abuse material. The UNODC report suggests that law enforcement efforts may be catching as little as 1% of all consumers of child sexual abuse materials.[216]

Arrest and prosecution data are likely to be more indicative of the resources made available to law enforcement to combat this criminal activity, rather than an indication of the number of consumers of child sexual abuse material.

Payment Disruption

The Financial Coalition Against Child Pornography was established in 2006 and involves 35 financial institutions and Internet industry bodies, along with the US National Centre for Missing and Exploited Children and its sister organisation, the International Centre for Missing and Exploited Children. Members include the Bank of America, Citigroup, Deutsche Bank, Google, HSBC – North America, Microsoft, Mastercard, Paypal, Visa, Western Union and Yahoo!. As a result of their efforts to block financial transactions involving commercial child sexual abuse site online, some of these sites are now refusing to process credit card payments from the US.

An Asia-Pacific Financial Coalition Against Child Pornography was established in 2009 and is based in Singapore. All providers of Australian merchant facilities for credit cards are involved in the Asia-Pacific Financial Coalition Against Child Pornography through the Australia card Risk Council being a member.

However, new alternative payment systems are being developed that offer increased anonymity for both purchasers and purveyors of illegal content in that many require little or no information about either the buyers or sellers utilizing the new payment systems. Unlike more established payments systems and services, these outfits are often willing to facilitate payments between parties with no record of, or interest in, any information about the parties' identities, legitimacy, or legality. As such, the emerging payment systems offer an appealing transaction option for illicit goods and services, including child sexual abuse images.[217]

The Financial Coalition Against Child Pornography report for several years there is an increasing sophistication on the part of commercial child sexual abuse businesses with

[215] Virtual Global Taskforce Media Release, 'VGT Board of Management Meeting Communique: September 2011', 26 September 2011, http://www.virtualglobaltaskforce.com/
[216] UNODC, *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* on 17 June 2010
[217] Financial Coalition Against Child Pornography, 'Report on Trends in Online Crime and Their Potential Implications in the Fight Against Commercial Child Pornography', 1 February 2011, p. 2.

regards to screening buyers. An ever increasing number of technical hurdles, including offline purchase validation and leveraging legitimate website affiliate programs to mask child sexual abuse material purchases, have been put in place most likely to flag undercover law enforcement credit card transactions.[218] At the same time, consumers of commercial child sexual abuse materials have been increasingly able to steal or purchase real identities of others to also hide from law enforcement. This also places innocent people at risk of being suspected of purchasing of child sexual abuse material, where their identity has been used by an offender for that purpose.[219]

Disrupting Searches for Child Sexual Abuse Material

UK Prime Minister David Cameron has put pressure on Google, Bing (owned by Microsoft) and Yahoo to stop assisting people trying to access images of child sexual abuse, "There are some searches which are so abhorrent and where there can be no doubt whatsoever about the sick and malevolent intent of the searcher that there should be no search results returned at all…. I simply don't accept the argument that some of these companies have used to say that these searches should be allowed because of freedom of speech."

Google and Microsoft have given in to the pressure and will introduce software to block 100,000 search terms that are clearly used only to find child sexual abuse material online. They will also stop the auto-complete feature from prompting users with child sexual abuse search terms even if the person was not looking for them. A further 13,000 search terms linked with child sexual abuse will flash up with warnings to users that the content could be illegal, and pointing them towards help. Google and Microsoft cover 95% of users.

These measures will also cover Australian users. We urge the Australian Government to actively support the requirement that searches for child sexual abuse material be disrupted.

Prime Minister David Cameron stated the UK National Crime Agency will monitor the effectiveness of the new technology introduced by Google and Microsoft and "If the search engines are unable to deliver on their commitment to prevent child abuse material being returned from search terms used by paedophiles. I will bring forward legislation that will ensure it happens."

Global Alliance

The Unit welcomes the Australian Government having committed to join the Global Alliance against child sexual abuse online, which was launched on 5 December 2012.[220] To date Ministers from 48 countries are participating. The Global Alliance undertakes work to identify and protect child victims, investigate cases and prosecute offenders, increase awareness risks for children online and reduce the availability of child sexual abuse material online. Each participating government states what the current situation in their country is and what future steps they will be taking. They are to report back in two years what progress has been made towards those goals.[221] The Global Alliance will also strengthen efforts to make sure the INTERPOL international database of detected and identified child abuse material grows by 10% annually and to make it easier to initiate joint cross-border police investigations.[222]

---

[218] Financial Coalition Against Child Pornography, 'Report on Trends in Online Crime and Their Potential Implications in the Fight Against Commercial Child Pornography', 1 February 2011, p. 3.
[219] Financial Coalition Against Child Pornography, 'Report on Trends in Online Crime and Their Potential Implications in the Fight Against Commercial Child Pornography', 1 February 2011, p. 3.
[220] European Commission Memo, 'Combating sexual abuse of children online: a Global Alliance for greater results', http://europa.eu/rapid/press-release_MEMO-12-937_en.htm, 4 December 2012.
[221] European Commission Memo, 'Combating sexual abuse of children online: a Global Alliance for greater results', http://europa.eu/rapid/press-release_MEMO-12-937_en.htm, 4 December 2012.
[222] Cecilia Malmstrom and Eric Holder, 'Ending an online scourge', The Age, 4 December 2012.

6.3 Areas for further action by Australia

We completely agree with the Prime Minister, The Hon Tony Abbott, that, "As a community we must have zero tolerance for the sexual abuse of children. Wherever abuse has occurred it must be tackled and it must be tackled vigorously, openly and transparently."[223] We strongly believe this also applies to children overseas who have been sexually abused and whose images have either been traded or purchased by Australians online.

Rehabilitation of Offenders

Australia could be doing much more to rehabilitate offenders who have purchased images of child sexual abuse, without having committed contact offences, to reduce recidivism.

The effectiveness of interventions with non-contact offenders is borne out by the lower reconviction rates of these offenders compared to contact offenders.[224] Seto and Eke (2005) conducted a study of a sample of 201 Canadian adult male offenders for child sexual abuse material offences. They found that in a three year period (April 2001 to April 2004) the recidivism rate for non-contact offenders was lower than for those who also had contact offences (3.9% compared to 5.3%). Those with only offences related to viewing child sexual abuse material were far less likely to reoffend with a contact offence than those with a past history of sexual contact offences (1.3% compared to 9.2%).[225] A Swiss study of 231 offenders, for an average of 7.5 years, found only 11 went on to commit another offence, of which only two involved physical contact with a child.[226] Webb *et al.* (2007) examined 73 offenders related to child sexual abuse material and found only 4% failed to adhere to the conditions of community supervision and none were charged with new offences during 18 months of supervision.[227]

Use of 'Stop' messages

This lower rate of recidivism amongst non-contact offenders and their ability to be persuaded to empathise with the victims of the abuse they are viewing, points to the value of access disruption by ISPs. Use of a block message provides an educative moment to challenge the cognitive distortions of the non-contact offender. Informal discussions with law enforcement officials who work to combat child sexual abuse online indicate that education of offenders and potential offenders is a vital tool. However, to our knowledge there are no wide scale education campaigns targeting this group. While the Australian Federal Police are engaging with academia and non-government organisations on the issue of offender education, they are not currently engaged in any education program specifically targeted at online offenders.[228]

With the right message on a 'stop' page that pops up when an attempt is made to access child sexual abuse material it can remind the offender what they are attempting to do is illegal and may help undermine the process of normalisation and cognitive distortion offenders use to justify their behaviour. The International Telecommunications Union

[223] The Hon Tony Abbott MHR, Media Release, "The sexual abuse of children", 12 November 2012.
[224] J. Osborn, I.A. Elliott, D. Middleton and A.R. Beech, *The use of actuarial risk assessment measures with UK internet child pornography offenders*, J. of Aggression, Conflict and Peace Research **2(3)** (2010), p.16.
[225] M.C. Seto and A.W. Eke, *The Criminal Histories and Later Offending of Child Pornography Offenders,* Sexual Abuse: A Journal of Research and Treatment **17(2)** (2005), p. 207.
[226] J. Endrass, F. Urbaiok, L.C. Hammermeister, C. Benz, T. Elbert, A. Lauerbacher and A Rossegger, *The Consumption of Internet child pornography and violent sex offending,* BMC Psychiatry **9** (2009), p. 43.
[227] L. Webb, J. Craissati and S. Keen, *Characteristics of Internet child pornography offenders: A comparison with child molesters*, Sexual Abuse **19** (2007), pp. 449-465.
[228] Senate Estimates Hansard, Assistant Commissioner Neil Gaughan, Australian Federal Police, 18 October 2011.

highlighted the educative value of block pages when a list is used by ISPs to disrupt the commercial child sexual abuse industry online:[229]

> *When a site is blocked, a STOP page should be displayed to the user. This STOP page has the dual function of giving information as to the reason the site was blocked (illegality of content) plus acting as a prevention vehicle that reminds the user/ consumer of the illegal nature of the material, as well as the presence of law enforcement agencies online.*

A 'stop' page serves as an educational moment for offenders. Research has shown that many offenders who buy child sexual abuse material (but who do not physically abuse children themselves) believe they are doing nothing wrong because access to such material is not challenged. Because there is ready availability of such material on the Internet, this view is reinforced. Access disruption by ISPs challenges this view.

The 'stop' page may also refer to them to services where they can seek help. There are certainly examples of offenders who have sought assistance to address their accessing of child sexual abuse material, without having been detected by law enforcement officials.[230]

Preservation of Evidence online

There is a need for the preservation of evidence in the investigation of cases involving online child sexual abuse. As noted by the Australian Institute of Criminology:[231]

> *The modern criminal, using the same devices as today's teenagers, communicates with Voice over Internet Protocol, video instant messaging, cellular camera phone, and text messaging in computer slang that is foreign to most police officers and parents. The trail to uncover this valuable investigation resource often starts with a forensic examination, but this trail quickly grows cold as Internet Service Providers overwrite logs and data retention periods expire. All police agencies are facing the same challenge when dealing with computer forensics. Police managers must find a way to examine an increasing number of digital devices, each containing an immense volume of data, in a timely manner and with limited resources.*

Need for Research

Further research is needed to determine the typology and behaviour of Australian consumers of child sexual abuse material. The Australian Government also needs work with other governments and UN bodies to research the business models of commercial producers of child sexual abuse material to determine additional measures to disrupt their businesses.

International Co-operation on Law Harmonisation

Currently, a majority of countries have inadequate laws in place to deal with online child sexual abuse. Due to the transnational nature of this criminal activity, the Australian Government needs to work with other countries to harmonise laws dealing with child sexual abuse material online.

---

[229] International Telecommunications Union, 'Guidelines for Policy Makers on Child Online Protection', 2009, p. 29.

[230] Olav Nielssen, Jeremy O'Dea, Danny H Sullivan, Marcelo Rodriguez, Dominique Bourget and Matthew M Large, *Child pornography offenders detected by surveillance of the Internet and by other methods*, Criminal behaviour and mental health 21(3) 2011, pp. 215-224

[231] Kim-Kwang Raymond Choo, 'Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences' Australian Institute of Criminology Research and Public Policy Series 103, 2009, p.82.

The International Centre for Missing & Exploited Children provides an assessment of legislation against child sexual abuse material globally.[232] They specifically examined if national legislation:

- Exists with specific regard to child pornography, not just pornography in general;
- Provides a definition of child pornography;
- Expressly criminalises computer-facilitated offences;
- Criminalises possession of child pornography, regardless of intent to distribute; and
- Requires ISPs to report suspected child pornography to law enforcement or to some mandated agency.

They found that only 45 countries have legislation sufficient to combat child sexual abuse material (eight countries met all of the criteria above and 37 countries met all but the last criteria, pertaining to ISP reporting) and 89 countries continue to have no legislation at all that specifically addresses child pornography.[233]

Of those countries that do not have legislation specifically addressing child sexual abuse material:

- 52 do not define child pornography in national legislation;
- 18 do not explicitly provide for computer-facilitated offences; and
- 33 do not criminalise possession of child sexual abuse material, regardless of intent to distribute.

The International Telecommunications Union has also stressed the need for international harmonisation of laws against child abuse material online as a key step towards the success of any strategy for child online protection.[234] An assessment of takedown notices commissioned by the UK Internet Watch Foundation concluded "harmonising laws relating to online child sexual abuse content is essential for minimising the impact of different national standards on further development and effective implementation of an international notice and takedown system."[235]

Restitution payments to victims

In US it is possible for victims of child sexual abuse to seek restitution payments from people who have downloaded their images through a provision in the *Violence Against Women Act*.[236] The payments are for the costs of the harm caused to the victim knowing that images of the abuse are being downloaded. The Unit would support such a measure being introduced in Australia. This could be extended to online social media outlets that are negligent in preventing the uploading or removal of child sexual abuse material. Such payments assist victims to feel the crime against them is being taken seriously as well as providing a further deterrent to offenders distributing and viewing the material.

Role of Cyber-Safety Education

Education of Australian parents and children may serve an important role in promoting cyber safety for Australian children and may assist in reducing inadvertent access to child sexual abuse material online. However, this does nothing to protect children who are victims located overseas whose images are purchased by Australian offenders.

---

[232] International Centre for Missing & Exploited Children, http://www.icmec.org

[233] International Centre for Missing & Exploited Children, 'Child Pornography: Model Legislation & Global Review', 6th Edition, 2010, p.iii.

[234] International Telecommunications Union, 'Guidelines for Policy Makers on Child Online Protection', 2009, p. 21.

[235] Weixiao Wei, 'Online Child Sexual Abuse Content: The Development of a Comprehensive, Transferable International Internet Notice and Takedown System', UK Internet Watch Foundation, p. 2.

[236] Emily Bazelon, 'The Price of a Stolen Childhood', *The New York Times*, 24 January 2013.

Dr Mark Zirnsak
Director
Justice and International Mission Unit
Synod of Victoria and Tasmania
Uniting Church in Australia