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

Centre for Theology and Ministry
29 College Crescent
Parkville Victoria
Australia, 3052
Telephone: 0409 166 915
jim@victas.uca.org.au

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

Supplementary Submission by the Synod of Victoria and Tasmania, Uniting Church in Australia to the inquiry into the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*
29 March 2021

The Synod of Victoria and Tasmania, Uniting Church in Australia, welcomes this opportunity to provide a supplementary submission on the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* to provide a civil society perspective on how the powers in the Bill are needed to help protect human rights from serious criminal activity facilitated by the online world.

The supplementary submission addresses the following issues:
- Trust and mistrust in the AFP, ACIC, judges, AAT members and magistrates;
- What offences should the powers in the Bill be allowed to be used for to investigate or prevent the offence;
- The need for the ability to issue emergency disruption warrants; and
- The complexity of defining innocent parties.

Trust in the AFP, ACIC, judges, AAT members and magistrates

Overwhelmingly, the evidence is that the AFP use the powers granted to them as intended and appropriately to the severity of the crimes they have been tasked with addressing. The examples of the AFP inappropriately using their powers are few and far between. The Committee should not place blind trust in the AFP and the ACIC. However, the safeguards that need to be put in place should not be built on the assumption that members of the AFP and ACIC will misuse the powers granted to them if given any opportunity to do so.

Some of the submissions provided to the Committee work from the assumption that members of the AFP, ACIC, judges, AAT members and magistrates cannot be trusted and will not use common sense in the application of the powers. It is assumed that if a warrant can be sought for a particular offence, the AFP and ACIC will seek to gain such a warrant. Further, the judge, AAT member or magistrate that considers the application for the warrant cannot be relied upon to comply with considering the factors required of them in the Bill in granting the warrant.

The irrational and unjustified mistrust of law enforcement agencies is out of step with the broad Australian community. A survey conducted by Democracy 2025 conducted in May to June 2020

found trust in police amongst Australians was at 75%, just 2% behind trust in health services.[1] Trust in the judiciary lagged significantly behind, with only 55% of Australians expressing trust in the courts.[2]

Concern was raised about metadata being accessed for minor offences. However, as this Bill relates only to granting powers to the AFP and the ACIC, the Committee should only consider the APF and ACIC use of accessing metadata. In the evidence provided to the Committee, the AFP stated that since 13 April 2015 they had never accessed a person's telecommunications data in reliance on section 280 of the *Telecommunications Act* in conjunction with another law.[3]

The Law Council reported to the Committee that the AFP had accessed metadata in pursuit of offences related to illicit drugs, but was unable to provide any evidence that the offences in question were not serious offences.[4]

Seriousness of the Offence the Warrants should be available for

The Synod remains of the view that the warrants in the Bill should be available for offences that carry a maximum term of imprisonment of three years or more, in order to allow the AFP and ACIC flexibility in the pursuit of serious criminal activity. It is reasonable for the Committee to trust the AFP and ACIC will use the powers in the Bill to target serious crime, and not for lesser crimes that are unrelated to serious criminal conduct. Even if the AFP or ACIC attempted, on a rare occasion, to obtain a warrant for a lesser criminal matter there are still the safeguards in the Bill that the authorising judge, AAT member or magistrate (depending on the warrant) would need to be satisfied that the application met all the criteria outlined in the Bill.

Trying to list all the crimes that the new warrants should cover would be a massive undertaking, as it would require a review of all laws and an assessment of which would be considered to cover serous criminal conduct.

As outlined in evidence to the Committee, it is clear there are differences of opinion between the submitting bodies on what constitutes sufficient harm to people that the new powers should apply. If the Committee were to start to remove certain offences from those that the warrants could apply to, the Committee should seek to hear from parties that have been impacted by the crimes in question before deciding that a particular crime is not serious enough for the AFP and ACIC to be able to seek a warrant at all.

Article 2(b) of the UN Convention against Transnational Organised Crime defines serious crime as:

> *(b) "Serious crime" shall mean conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty;*

---

[1] Mark Evans, Viktor Valgardsson, Will Jennings and Gerry Stoker, 'Political Trust and Democracy in times of Coronavirus: Is Australia still the Lucky Country?', Democracy 2025, 2020, 4.
[2] Mark Evans, Viktor Valgardsson, Will Jennings and Gerry Stoker, 'Political Trust and Democracy in times of Coronavirus: Is Australia still the Lucky Country?', Democracy 2025, 2020, 4.
[3] Parliamentary Joint Committee on Intelligence and Security, 'Review of the mandatory data retention regime', 2020, 34, 73.
[4] Parliamentary Joint Committee on Intelligence and Security, 'Review of the mandatory data retention regime', 2020, 63.

Australia is a States Party to the Convention. Therefore the Committee should take into account this international obligation as part of its consideration of what threshold should apply to the offences a warrant can be applied for.

If the Committee were to recommend that the threshold for offences that the AFP and ACIC have discretion to apply for a warrant was to be increased it may cut off investigation into offences like the negligent laundering of any amount of proceeds of crime (which carries a maximum penalty of five years imprisonment).[5] Even under the current Bill, the AFP and ACIC would not be able to apply for a warrant for an offence of negligently laundering less than $50,000, which carries a maximum penalty of two years in prison.

As the Bill stands, no warrant could be applied for under s.478.1(1) of the Criminal Code for unauthorised access to, or modification of, restricted data, which only carries a maximum penalty of two years in prison. Such criminal activity may point to far more serious criminal activity behind the unauthorised access, but the warrants could not be used in relation to an investigation into this offence.

If the Committee recommends an increase in the threshold it could cut off the ability of the warrants to be used in cases to investigate abuse of public office, as s.142.2(1) Criminal Code carries a maximum penalty of five years in prison.

As it stands the warrants cannot be used to investigate cases of unlawful disclosure of information by Commonwealth officers under s.70(1) of the *Crimes Act 1914.*

The Committee has been presented with an argument by some submitting organisations that under no circumstances should the warrants be permitted to be sought for the unlawful removal of a child from Australia under s. 65Y of the *Family Law Act.* Australia has obligations under the Hague Convention on the Civil Aspects of International Child Abduction. The situations where the unlawful removal of a child from Australia by one parent can occur are complex. However, they can cause great distress to both the children and the parent who may not know where the children have been removed to. Such unlawful removals of children from Australia may be a violation of the human rights of the children in question. It is our understanding that the AFP almost never seek a prosecution under s. 65Y as it is usually not in the best interests of the children to have their parent imprisoned. However, it is further our understanding that there are cases where one parent removes the children from Australia and places them in the care of relatives overseas as a means to cause distress on the other parent, as a form of emotional family violence. We would therefore take the view that there may be circumstances where the AFP being able to use the powers in the Bill to locate children who have been removed overseas, especially where the safety or well-being of the children is under threat, may justify application for a warrant under the Bill. There are likely to be other circumstances, such as the parent who unlawfully removes the children from Australia is doing so to escape family violence being perpetrated against them and the children, where it would not be appropriate for the AFP to assist in the location of the children using the powers in the Bill. The point being, that the complexity of the situations that may arise can justify the warrants being available for the rare cases where their use would be justified. Further discussion of the complexities that may arise in such cases could be taken up with International Social Services Australia, should the

[5] https://www.cdpp.gov.au/crimes-we-prosecute/money-laundering

Committee wish to explore this area further. Further, the Senate Legal and Constitutional Committee conducted an inquiry into this issue in 2011, highlighting the distress and suffering that unlawful removal of children from Australia can cause.[6]

The Synod is of the view the Committee should not recommend a change to the threshold of when warrants can be applied for without a thorough analysis of the implications of denying the powers in the Bill would mean in relation to the offences then excluded. Such an analysis should take account of the impact on human rights and the impact on the natural environment (by the exclusion of offences related to serious environmental crimes) by excluding the use of the warrants for certain types of serious crime and human rights abuses.

The Synod believes that ss.134.1(1), 134.2(1) and 135.4(3) of the Criminal Code can relate to very serious criminal conduct that violate the human rights of the broader community by reducing available government resources to provide valuable services to the community. We strongly disagree with the Law Council of Australia that these offences cover criminal conduct "at the lower end of objective seriousness". As pointed out by the Australian Institute of Criminology, as of 30 June 2019, the AFP was investigating 105 fraud matters related to the Commonwealth Government worth over $1.2 billion.[7] Further, they estimated that 8% of Commonwealth agency resources are potentially affected by fraud.[8] There is a growing acceptance in broader civil society that tax crimes, including tax fraud, result in serious human rights violations. For example, a 2019 report by the Centre for Budget Governance Accountability, Christian Aid, Fundacion SES and the Financial Transparency Centre outlined how abusive tax practices against government revenue should be considered serious human rights abuses.[9]

As outlined in the Plutus Payroll tax fraud case outlined below, the ability of the AFP and ATO to stop the offending appears to have been impeded by the inability to establish the link between the straw directors of the shell companies those behind the criminal activity. Shutting down the tax fraud earlier may have prevented the theft of tens of millions of dollars in tax fraud. The Committee could verify the details of if the use of the powers in the Bill would have assisted the investigation with those involved in the investigation.

As a final comment, exclusion of certain offences from being subject to the warrants does not change the penalties available for those offences. It does create an environment in which offenders who have access to technological expertise are more likely to escape detection and prosecution, potentially allowing the criminal behaviour and associated human rights abuses to persist. It is likely offenders that have access to technological expertise are likely to be those that are more organized and are committing offences at the more serious end of the scale for

---

6 https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Completed_inquiries/2010-13/childabduction/report/index

7 Coen Teunissen, Russell Smith and Penny Jorna, 'Commonwealth fraud investigations 2017-18 and 2018-19', Australian Institute of Criminology, AIC Statistical Report 25, 2020, x.

8 Coen Teunissen, Russell Smith and Penny Jorna, 'Commonwealth fraud investigations 2017-18 and 2018-19', Australian Institute of Criminology, AIC Statistical Report 25, 2020, x.

9 Matti Kohonen, Abena Yirenkyiwa Afari, Attiya Waris, Marcos Lopes-Filho, Mike Lewis, Neeti Biyani, Sakshi Rai, Tomas Julio Lukin and Uddhab Pyakurel, 'Trapped in Illicit Finance. How abusive tax and trade practices harm human rights', Christian Aid, Centre for Budget Governance Accountability, Fundacion SES and the Financial Transparency Coalition, September 2019.

that particular crime. Making sure that only minor offences are possibly detectable can then act as a shield against law enforcement agencies being able to access the powers in the Bill. As outlined below, using shell companies with straw directors may be even more attractive if the crime in question allows for such an arrangement. The straw director may have only committed more minor offences, which are detectable and conceal the more serious offences underneath.

The need for the ability to issue emergency data disruption warrants

The Synod believes that there will be situations vital to the protection of human rights where the AFP will need the ability to carry out an emergency authorisation of a data disruption warrant. For example, an offender is about to conduct a live webcam child sexual abuse session where they would be issuing the instructions on what abuse should be inflicted on the child. The data disruption warrant would allow the AFP to prevent the abuse from occurring. We strongly disagree with other submitting bodies that the AFP should be impeded from preventing such abuse from occurring in the very rare circumstances where there is insufficient time to follow the normal process of obtaining a data disruption warrant. We are of the view that the use of the emergency authorisations will be exceedingly rare. The Synod would support a review of the use of the emergency authorisations after three years to ensure that they are being used appropriately by the AFP and ACIC.

The Complexity of Defining Innocent Third Parties

There is substantial complexity to defining 'innocent' third parties. The reality is that there is spectrum of the ways people may be connected to criminal activity and human rights abuses facilitated online. The spectrum can include:

- The offender;
- A person knowingly facilitating the actions of the offender;
- A person recklessly or negligently facilitating the actions of the offender, but who may lack knowledge of the offending or human rights abuses and may not be guilty of an offence themselves through their behaviour;
- A person who has been deceived into assisting the offender in their activities and who may have no knowledge of the offending or human rights abuses;
- A person whose identity has been stolen and is being used to carry out the criminal activity. In some cases the person's computer may also be hijacked without their knowledge and used to perpetrate serious crimes and human rights abuses; and
- Innocent third parties that have no association with the crime or human rights abuses associated with the criminal activity.

Thus, it would be flawed to design the Bill around a flawed binary concept that there are only offenders and third-party non-suspects.

Therefore, as an example, Recommendation 9 of the Law Council of Australia submission that there be an absolute prohibition on the AFP and ACIC doing acts or things that are likely to cause material loss, in any amount, or damage to third-party computer users, who are not suspects or persons of interest in an investigation or operation places an unreasonable restriction on the use of the powers.

Consider the case of Liberty Reserve. In the case, US authorities sought to seize the assets in three Westpac accounts held by Technocash Ltd holding up to $36.9 million.[10] Technocash Limited was an Australian registered company. The funds were alleged to have been connected to shell companies owned by the defendants in the case.[11] 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 users 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:[12]

> *…intentionally created, structured, and operated Liberty Reserve as a criminal business venture, one designed to help criminals conduct illegal transactions and launder the proceeds of their crimes. Liberty Reserve was designed to attract and maintain a customer base of criminals by, among other things, enabling users to conduct anonymous and untraceable financial transactions.*
>
> *Liberty Reserve emerged as one of the principal means by which cyber-criminals around the world distributed, stored and laundered the proceeds of their illegal activity. Indeed, Liberty Reserve became a financial hub of the cyber-crime world, facilitating a broad range of online criminal activity, including credit card fraud, identity theft, investment fraud, computer hacking, child pornography, and narcotics trafficking. Virtually all of Liberty Reserve's business derived from suspected criminal activity.*
>
> *The scope of Liberty Reserve's criminal operations was staggering. Estimated to have had more than one million users worldwide, with more than 200,000 users in the United States, Liberty Reserve processed more than 12 million financial transactions annually, with a combined value of more than $1.4 billion. Overall, from 2006 to May 2013, Liberty Reserve processed an estimated 55 million separate financial transactions and is believed to have laundered more than $6 billion in criminal proceeds.*

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.[13]

US authorities alleged defendant Arthur Budovsky used Technocash to receive funds from exchangers. Mr Budovsky, the alleged principal founder of Liberty Reserve,[14] allegedly used his bank to wire funds to Technocash bank accounts held by Westpac.[15] He was also alleged to be the registered agent for Webdata Inc which held an account with SunTrust. Technocash records allegedly showed deposits into the SunTrust account from Technocash accounts associated with Liberty Reserve between April 2010 and November 2012 of more than $300,000.[16]

---

[10] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 29, 43.
[11] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 21.
[12] US Attorney for the Southern District of New York, 13 Civ 3565, 28 May 2013, pp. 4-5.
[13] US Attorney for the Southern District of New York, 13 Civ 3565, 28 May 2013, p. 6.
[14] 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.
[15] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 29.
[16] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 36.

Arthur Budovsky was allegedly listed as the president for Worldwide E-commerce Business Sociedad Anonima (WEBSA) and defendant Maxim Chukharev as the secretary. Maxim Chukharev was alleged to have helped design and maintain Liberty Reserve's technological infrastructure.[17] 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.[18] It was 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.[19]

It was alleged Arthur Budovsky was the president of Grupo Lulu Limitada which was allegedly used to transfer and disguise Liberty Reserve Funds.[20] 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.[21]

Further, defendant Azzeddine El Amine, manager of Liberty Reserve's financial accounts,[22] was the Technocash account holder for Swiftexchanger. It was 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 2012 and 1 May 2013, exchangers doing business with Liberty Reserve send approximately $36,919,884 to accounts held by Technocash at Westpac.[23]

The defendants were alleged to have used Technocash services to transfer funds to nine Liberty Reserve controlled accounts in Cyprus.[24]

Arthur Budovsky was sentenced to 20 years in prison for the offences related to Liberty Reserve in May 2016. The court noted that his crimes caused "widespread harm" and led to "countless victims of fraud around the world". Maxim Chukharev pled guilty and was sentenced to three years in prison.[25] Azzeddine El Amine pled guilty and was sentenced in May 2016 to time served.[26]

---

[17] 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.
[18] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 37.
[19] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 36.
[19] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 38.
[20] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 36.
[20] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 40.
[21] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 36.
[21] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 41.
[22] 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.
[23] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 30.
[24] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 31.
[25] US Attorney's Office, Southern District of New York, 'Liberty Reserve Founder Arthur Budovsky Sentenced In Manhattan Federal Court To 20 Years For Laundering Hundreds OF Millions Of Dollars

Technocash Limited was 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.[27] Technocash stated that it "complied with Australia's comprehensive AML regime, verified customers and has an AFSL licence since 2003. Technocash denied any wrong doing."[28]

If the legislation were to be amended as recommended by the Law Council, firstly in a case like Liberty Reserve, the AFP would be prohibited from conducting any data disruption action against Liberty Reserve if it carried the risk of causing a loss to any person who was using Liberty Reserve and was not themselves involved in criminal activity regardless of the benefit to preventing further crime and human rights abuses such action may have. Further, the AFP or ACIC would have been prohibited from disrupting any transactions conducted by the people involved with Liberty Reserve involving Technocash if it would cause staff at Technocash any material loss, unless the AFP or ACIC could demonstrate that the staff working for Technocash who might suffer material loss were suspects in the criminal activities. Given Technocash claimed no knowledge of the criminal activity, such a threshold may prove insurmountable.

There has been an on-going trend of people involved in serious crime to use shell companies with straw directors and dummy owners to launder the proceeds of crime and facilitate other criminal conduct. If the Law Council recommendation were adopted the use of data disruption warrants could be frustrated were a straw director or dummy owner to face the risk of suffering any material loss as a result of the use of the data disruption warrant, where the straw director or dummy owner had no knowledge of the criminal offending involved. It may encourage criminal operations to structure their activities to ensure that third parties are at risk of suffering material loss if a data disruption warrant is applied as way of frustrating the use of such warrants.

As examples of such cases, the ATO and AFP obtained the conviction of Philip Northam to six years in prison for tax evasion related offences in 2020. Australian companies were stripped of their assets and left in a position where they were unable to pay their tax debts. Once the assets of the company were stripped, new straw directors and shareholders were put in place before the company was wound up. The joint ATO and AFP investigation was able to recover $4.5 million of lost government revenue from the criminal conduct.[29]

In the case of the Plutus Payroll fraud the criminals involved set up a significant number of sheel companies with straw directors. One of the criminals involved had a full-time role to manage and control the straw directors.[30] Plutus issued false invoices to the shell companies and siphon out

---

Through His Global Digital Currency Business', 6 May 2016, https://www.justice.gov/usao-sdny/pr/liberty-reserve-founder-arthur-budovsky-sentenced-manhattan-federal-court-20-years

[26] Nate Raymond and Brendan Pierson, 'Digital currency firm co-founder gets 10 years in prison in US Case', Reuters, 14 May 2016, https://www.reuters.com/article/us-usa-cyber-libertyreserve-idUSKCN0Y42A2

[27] Technocash, 'Opportunity: Own the Technocash Payment Platform', Media Release, 5 July 2013.

[28] http://www.technocash.com/pages/press-release.cfm

[29] ATO, '19-year tax fraud probe ends in jail time for scheme promoter', 17 August 2020, https://www.ato.gov.au/Media-centre/Media-releases/19-year-tax-fraud-probe-ends-in-jail-time-for-scheme-promoter/

[30] Cactus Consulting, 'Plutus Payroll Case Study; Significant tax fraud', 26 November 2019.

the PAYG not paid on behalf of the client companies using its payroll service.[31] To try to escape action by the ATO, the shell companies would be wound up and replaced with a new shell company with a new straw director.[32] It was found that Devyn Hammond would sign off on records in place of the straw directors and impersonate them in e-mails.[33] The scheme allegedly defrauded the Commonwealth Government of $105 million over three years.[34] As of July 2020, 16 people had been charged in relation to the criminal conduct and five had been sentenced to prison.[35] Again, it is possible that a number of the straw directors were not aware of criminal activity being carried out. In such a case, the use of a data disruption warrant could be frustrated if the action would cause material loss to a straw director unaware of the criminal activity. Assessment of the case suggests that the investigation lasted for as long as it did because the law enforcement agencies were frustrated in being able to establish the link between the criminals behind the scheme and the straw directors.[36]

Geelong baker Barry Santoro allegedly had his identity stolen and was convicted of corporations offences for companies he did not know he was the director of. He was one of a number of people, including people who were homeless, who were allegedly used as straw directors to allow the real beneficial owners of the companies to cheat the tax office and other creditors of more than $100 million.[37] The alleged scheme involved stripping businesses of their cash and assets in order to cheat the tax office and other creditors, and then phoenixing under a different name. the straw directors were installed to shield the real directors from liquidators, creditors and ASIC.[38] In the same scheme, Christopher Somogyi, who had been homeless at the time, was fined more than $6 million through director penalty notices and other fines after his identity was allegedly used without his knowledge as a straw director for a number of companies.[39]

The Age reported in October 2020 of an Australian lawyer that advises clients to use Seychelles' private foundations to conceal the true ownership of companies and conceal activities from law enforcement agencies. He was quoted as advising "In the event of a lawsuit or tax investigation or regulatory inquiry, your client can swear under oath, 'I am not the legal or beneficial owner of this company', which could be the difference between being charged with/ jailed for tax evasion and walking away a free man."[40] Again, it is possible that the use of data disruption warrants may result in material loss to those businesses that recklessly, but legally, supply shell companies to criminals to carry out their activities and frustrate law enforcement

[31] Cactus Consulting, 'Plutus Payroll Case Study; Significant tax fraud', 26 November 2019.
[32] Cactus Consulting, 'Plutus Payroll Case Study; Significant tax fraud', 26 November 2019; and David Marin-Guzman, ''Architect' of Plutus tax fraud pleads guilty', *The Australian Financial Review,* 26 November 2019.
[33] David Marin-Guzman, 'Fourth Plutus tax fraud conspirator sentenced to jail', *The Australian Financial Review,* 10 July 2020.
[34] ATO, 'Plutus Payroll founder jailed in Operation Elbrus', 31 July 2020.
[35] ATO, 'Plutus Payroll founder jailed in Operation Elbrus', 31 July 2020.
[36] Cactus Consulting, 'Plutus Payroll Case Study; Significant tax fraud', 26 November 2019.
[37] Dan Oakes,' Bake made director of companies he'd never heard of in $100m tax scam, court hears', ABC News, 27 August 2018.
[38] Dan Oakes,' Bake made director of companies he'd never heard of in $100m tax scam, court hears', ABC News, 27 August 2018.
[39] Dan Oakes,' Bake made director of companies he'd never heard of in $100m tax scam, court hears', ABC News, 27 August 2018.
[40] Nick McKenzie, Charlotte Grieve and Joel Tozer, 'Lawyer who built a booming practice on finding loopholes', *The Age,* 20 October 2020.

investigations.

Further, there may be cases where actions by the AFP could cause material loss to a person who is not a suspect or a person of interest, but whose identity is being misused by the criminals. So at the same time as the AFP action could cause immediate material loss, it may at the same time be providing protection from a greater harm being inflicted on the person by the criminals. If the Law Council recommendation is adopted any benefit of the AFP action would have to be disregarded if the action at the same time caused a material loss to the person. Such cases may arise where the criminals are using the computers of innocent third parties as zombie bots in the criminal activity.[41] In March 2020, a network of nine million zombie bots being used for criminal activity was shut down.[42] In October 2020, it was reported in the media that Microsoft took legal action to try to shut down a zombie bot network of one million computers being hijacked for serious criminal activity.[43] The AFP shut down the use of the Imminent Monitor Remote Access Trojan in November 2019, which was being used to create zombie bots with the computers of Australians and others for serious criminal activities by a global network of criminals.[44]

Dr Mark Zirnsak
Senior Social Justice Advocate
[redacted]

[41] For background on the use of zombie bot networks for serious criminal activity see Kim-Kwang Raymond Choo, 'Zombies and botnets', Australian Institute of Criminology Trends and Issues No. 333, March 2007.
[42] 'Microsoft takes down global zombie bot network', BBC News, 11 March 2020, https://www.bbc.com/news/technology-51828781
[43] Frank Bajak, 'Microsoft attempts takedown of global criminal botnet', AP, 13 October 2020.
[44] Australian Federal Police, 'The Rat Trap: international cybercrime investigation shuts down insidious malware operation', 30 November 2019.